Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ВОВК ОЛЕСЯ ОЛЕГІВНА

УДК 621.391

МЕТОДИ ПІДВИЩЕННЯ СТІЙКОСТІ ТА ПРОПУСКНОЇ ЗДАТНОСТІ СИСТЕМ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ

05.12.02 – Телекомунікаційні системи та мережі

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2016

Дисертацією є рукопис.

Робота виконана в Харківському національному університеті радіоелектроніки Міністерства освіти і науки України

Науковий керівник: кандидат технічних наук, доцент
Астраханцев Андрій Анатолійович,
Харківський національний університет радіоелектроніки Міністерства освіти і науки України,
доцент кафедри мереж зв'язку.

Офіційні опоненти: доктор технічних наук, професор
Кузнецов Олександр Олександрович,
Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України,
професор кафедри безпеки інформаційних систем і технологій;

кандидат технічних наук, доцент
Штомпель Микола Анатолійович,
Український державний університет залізничного транспорту Міністерства освіти і науки України,
доцент кафедри транспортного зв'язку.

Захист відбудеться « 07 » вересня 2016 р. о 13:00 годині на засіданні спеціалізованої вченої ради Д 64.052.09 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14.

Автореферат розісланий « 05 » липня 2016 р.

Учений секретар
спеціалізованої вченої ради О.Б. Ткачова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Обмеження на використання криптографічних засобів у ряді країн світу та виникнення проблеми захисту прав власності на інформацію, представлену в цифровому вигляді зумовлюють популярність досліджень у сфері стеганографії. Методи стеганографії дозволяють не тільки приховано передавати дані (так звана класична стеганографія), але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних і т. і. Ці обставини дозволяють у рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати важливі питання захисту інформації ряду прикладних галузей.

Робота присвячена розробці методу передачі прихованої інформації та цифрових водяних знаків (ЦВЗ), що є стійким до спотворень в каналах зв'язку та має високу пропускну здатність без втрат стійкості та рівня прихованості. Найбільш затребуваними в останні роки є методи захисту авторських прав на електронну продукцію та системи електронного захищеного документообігу (системи електронної нотифікації документів). Особливістю цих систем є передача прихованої інформації (у тому числі ЦВЗ) існуючими каналами зв'язку з завадами. Для цих систем розпізнавання та вилучення прихованої інформації є ключовим фактором, тому чутливість до спотворень та втрат пакетів при передачі в телекомунікаційних мережах значно впливає на якість та характеристики всієї системи прихованої передачі інформації. Для забезпечення додаткової завадостійкості необхідно забезпечити підвищення пропускної здатності, оскільки використання методів завадостійкого кодування чи дублювання інформації вимагає передачі додаткових біт.

Таким чином, є актуальною тема дисертаційних досліджень, направлених на підвищення завадостійкості та пропускної здатності систем прихованої передачі інформації, що використовують телекомунікаційні системи.

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

Проведення дисертаційних досліджень пов'язане з виконанням планових наукових досліджень Харківського національного університету радіоелектроніки, у рамках яких була виконана НДР № 276-4 «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку» (№ 0113U000360), в якій дисертант був виконавцем.

Метою дисертаційної роботи є підвищення ефективності систем прихованої передачі інформації у телекомунікаційних системах на основі стеганографічного методу з високими показниками стійкості та пропускної здатності. Для розв'язання наукової задачі в дисертаційній роботі розв'язані наступні окремі задачі дослідження:

– аналіз існуючих методів та засобів стеганографічного захисту інформації в МЗ (мережах зв’язку) і визначення якостей, що впливають на стійкість даних, що вбудовуються;

– аналіз та адаптація узагальненої математичної моделі та методів вбудовування даних у зображення;

– розроблення методики багатокритеріальної оптимізації з метою підвищення ефективності використання мереж зв’язку для прихованої передачі інформації;

– оптимізація якості функціонування телекомунікаційних систем прихованої передачі інформації;

– удосконалення стеганографічного методу вбудовування даних у вейвлет-коефіцієнти зображень з використанням частотного методу Коха-Жао;

– дослідження методів адаптації телекомунікаційних систем передачі прихованої інформації до зовнішніх впливів, та розроблення на цій основі методу підвищення захищеності та стійкості систем зв'язку;

– удосконалення процесу перетворення сигналів у телекомунікаційних системах для підготовки інформації до прихованої передачі мережами зв’язку;

– розробка та програмна реалізація методу підвищення стійкості стеганографічних систем до геометричних атак;

– розроблення методики визначення оптимальних параметрів дискретного вейвлет-перетворення для стеганографічних методів передачі інформації мережами зв’язку;

– розроблення стеганографічного методу вбудовування даних у нерухомі зображення, що забезпечує захищеність, надійність системи та підвищує ймовірність правильного розпізнавання вкладених даних;

– розробка програмного засобу для стеганографічного захисту інформації в МЗ та впровадження результатів і перевірка на практиці їх ефективності.

Об’єкт дослідження – процес обробки, захисту та прихованої передачі інформації в телекомунікаційних системах та мережах.

Предмет дослідження – математичні моделі, методи та засоби забезпечення стеганографічної стійкості телекомунікаційної системи до атак та завад у каналах зв’язку.

Методи дослідження. Розробка математичної моделі процесу стеганографічних перетворень інформації з урахуванням дії завад в каналах зв’язку здійснювалася на основі методів теоретико-множинного підходу. Підготовка інформаційного сигналу та сигналу-контейнера для вбудовування прихованих даних проводилася з використанням методів цифрової обробки сигналів та зображень. Для підвищення завадостійкості інформації використовувались методи теорії кодування. Для вибору оптимального за зазначеними критеріями методу застосовувалися методи багатокритеріальної оптимізації.

Наукова новизна отриманих результатів. При розв’язанні сформульованої наукової задачі у роботі отримано нові наукові результати:

1) Вперше отримано кількісні значення багатокритеріального аналізу стеганографічних методів з використанням комплексного критерію оцінювання стеганографічних систем, що на відміну від існуючих, враховують вимоги до методів вбудовування в залежності від призначення системи з урахуванням важливості показників якості. Це дало можливість сформувати вимоги щодо характеристик стеганографічних систем для підвищення загальної ефективності прихованої передачі інформації.

2) Удосконалено стеганографічний метод вбудовування даних у вейвлет-коефіцієнти зображень, відмінною особливістю якого є інтеграція принципів частотного методу Коха-Жао, розширення діагоналі вбудовування та використання двох матриць вейвлет-перетворення (HL та LH) для приховування повідомлення. Це дозволило досягти підвищення ефективності та загального виграшу у пропускній здатності системи у порівнянні зі стеганографічними методами на основі перетворень.

3) Удосконалено метод попередньої підготовки інформації до прихованої передачі телекомунікаційними системами, відмінною особливістю якого є обробка сигналів із послідовним застосуванням завадостійкого кодування, чергування та скремблювання, і методи адаптації телекомунікаційних систем передачі прихованої інформації до зовнішніх впливів, відмінною особливістю яких є використання дублювання міток та м’якого детектування. Це дало можливість підвищення захищеності та стійкості систем зв'язку.

4) Удосконалено метод підвищення стійкості стеганографічних систем до геометричних атак, що відрізняється вбудовуванням реєстраційного шаблону разом із цифровим водяним знаком. Це дозволяє підвищити стійкість до атак проти стеганографічного детектора на основі афінних перетворень (обрізка та повороти).

5) Вперше розроблено стеганографічний метод вбудовування даних у нерухомі зображення на основі послідовного застосування дискретного косинусного та дискретного вейвлет-перетворення, який, на відміну від існуючих, використовує удосконалені методи підвищення стійкості стеганографічних систем до геометричних атак та попередню обробку сигналів, що підлягають вбудовуванню. Це забезпечує стійкість, захищеність, підвищує ймовірність правильного детектування вкладених даних та дозволяє збільшити пропускну здатність системи.

Практична значимість дисертаційної роботи полягає в наступному:

1. Запропонований комплексний критерій оцінювання стеганографічних систем передачі інформації може бути використаний для вибору оптимального методу прихованої передачі інформації, в залежності від умов передачі та сфери застосування системи.

2. Рекомендації щодо вибору ефективного методу для побудови стеганографічної системи, дозволяють підвищити ефективність роботи системи

прихованої передачі інформації, зокрема надають можливості для більш раціонального використання пропускної здатності контейнерів, застосовані при виконанні НДР № 276-4 «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку», що підтверджено відповідним актом впровадження від 18.04.2016 р.

3. Використання запропонованих методів завадостійкого кодування, чергування та адаптації телекомунікаційних систем передачі прихованої інформації до зовнішніх впливів, дозволяє підвищити якість послуг, що надаються системою прихованої передачі інформації.

4. Отримані результати впроваджені в навчальний процес Харківського національного університету радіоелектроніки, зокрема, на кафедрі мереж зв'язку та кафедрі телекомунікаційних систем. Розроблений стеганографічний метод вбудовування даних у нерухомі зображення використано у дисципліні «Захист інформації у телекомунікаційних системах» (тема: «Методи прихованої передачі інформації»), а також метод попередньої підготовки інформації до прихованої передачі телекомунікаційними системами, що включає обробку сигналів із послідовним застосуванням завадостійкого кодування, чергування та скремблювання, використано у дисципліні «Теорія електричного зв'язку» (теми «Аналіз завадостійкості систем», «Теорія кодування»). Удосконалений стеганографічний метод вбудовування даних у вейвлет-коефіцієнти та метод підвищення стійкості стеганографічних систем до геометричних атак впроваджені в навчальний процес кафедри телекомунікаційних систем зокрема, у дисципліну «Основи стеганографічного захисту інформації» (тема «Методи вбудовування інформації у нерухомі зображення»). Це підтверджено відповідним актом впровадження від 18.04.2016 р.

Особистий внесок здобувача. Всі результати, які складають основний зміст дисертаційної роботи, здобувач отримав самостійно. У роботах, написаних у співавторстві, автору належать: [1] – оцінка стійкості і надійності методів приховування інформації в просторовій області нерухомих зображень; [2] – оцінка характеристик методів вбудовування на основі НЗБ при використанні завадостійкого кодування на тлі адитивної гаусівської завади; [3] – вирішення задачі оцінювання важливості (ваги) характеристик методів стеганографії; [4] – експериментальні дослідження характеристик методів прихованої передачі даних на основі вейвлетів; [5] – розробка методу вбудовування інформації у нерухомі зображення; [6] – синтез нового метод вбудовування інформації у нерухомі зображення; оцінка можливості методів адаптуватись до характеристик реальних каналів зв'язку; [7] – визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів.

Апробація результатів дисертації. Основні результати дисертаційного дослідження оприлюднено в ході 14 наукових конференцій, форумів і конкурсів, серед яких: V Міжнародна науково-практична конференція «Сучасні проблеми і

досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій», 2010 р. (Запоріжжя, ЗНТУ); Всеукраїнський конкурс студентських наукових робіт (галузь знань «Телекомунікаційні системи та мережі», «Інформаційні мережі зв'язку»), 2011 р. (Одеса, ОНАЗ); 15-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті», 2011 р., 2015 р., 2016 р. (Харків, ХНУРЕ); Міжнародна науково-практична конференція молодих вчених «Інфокомунікації – сучасність та майбутнє», 2011 р. (Одеса, ОНАЗ); Підсумкова науково-практична конференція Всеукраїнського конкурсу студентських наукових робіт (галузь знань «Інформаційна безпека»), 2012 р. (Львів, ЛП); 9-а Міжнародна молодіжна науково-технічна конференція «Сучасні проблеми радіотехніки і телекомунікацій РТ-2013», 2013 р. (Севастополь, СевНТУ); 23-а Міжнародна Кримська конференція «НВЧ-техніка і телекомунікаційні технології», 2013 р. (Севастополь, СевНТУ); Перша Міжнародна науково-практична конференція «Проблеми інфокомунікацій. Наука і технології», 2013 р. (Харків, ХНУРЕ); 13-а Міжнародна конференція «Modern problems of radio engineering, telecommunications, and computer science», 2014 р. (Славське, ЛП); Перша і друга Міжнародна науково-практична конференція «Problems of Infocommunications. Science and Technology», 2014 р., 2015 р. (Харків, ХНУРЕ); Всеукраїнська науково-практична конференція «Сучасні проблеми телекомунікацій та підготовка фахівців у галузі телекомунікацій – 2014», 2014 р. (Львів, ЛП).

Публікації. Основні положення і результати дисертаційної роботи знайшли своє відображення у 21 науковій роботі: 7 статей, з яких 6 в наукових фахових виданнях, затверджених МОН України [1-5, 7], 1 стаття [6] в іноземному виданні телекомунікаційної спрямованості; 14 публікацій матеріалів і тез доповідей на науково-технічних конференціях і форумах [8-21], з яких 4 конференції проходили під егідою IEEE [14, 16, 17, 20] і вкладені в науковометричних базах Scopus та IEEE Xplore Digital Library.

Структура та обсяг дисертаційної роботи. Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 174 сторінки, у тому числі 142 сторінки основного тексту, 56 рисунків, 23 таблиці, список використаних джерел із 126 найменувань, викладених на 13 сторінках.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЙНОЇ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, сформульовано основну мету і задачі дослідження, зазначено зв'язок результатів дисертаційної роботи з науковими програмами і темами, визначено об'єкт, предмет та методи дослідження, розкрито ступінь наукової новизни та рівень практичного значення результатів, отриманих у дисертаційній роботі.

У **першому розділі** надано обґрунтування необхідності розробки об’єктивної методики оцінювання стеганографічних методів, здатної забезпечити кількісні показники вибору оптимального методу прихованої передачі інформації в тих чи інших умовах.

Розглянуто можливості стеганографії при використанні для прихованого зв'язку, захисту авторських прав на зображення (автентифікації), відбитків пальців (відстеження порушника), тощо. Стверджується, що широкий спектр застосування та зростаючий попит обумовлюють актуальність підвищення стійкості та надійності прихованої передачі інформації по відкритих телекомунікаційних системах зв’язку саме за допомогою засобів стеганографії.

В роботі стеганографічна система розглядається як система прихованої передачі інформації. Де особлива увага приділяється блоку прекодера, що здійснює початкову обробку інформації, та стеганографічному каналу, що є каналом передачі контейнера-результата. Під час перебування у стеганографічному каналі контейнер, що містить приховане повідомлення, може піддаватися навмисним атакам або випадковим завадам.

Огляд наукових робіт показав, що існує велика кількість методів приховування даних саме у цифрових зображеннях, що обумовлено в першу чергу добре розробленими методами цифрової обробки зображень. Однак, саме це викликає й значні труднощі у забезпеченні стійкості ЦВЗ: чим сучаснішими стають методи компресії, тим менше залишається можливостей для вбудовування сторонньої інформації. Абсолютно зрозумілою є необхідність прийняття до уваги стеганометодами не тільки алгоритмів компресії зображень, але й властивостей зорової системи людини (ЗСЛ).

Зважаючи на поширеність, пов’язану з перевагами та недоліками різних типів, форматів і моделей цифрових зображень для досліджень були обрані растрові зображення формату *bmp* з глибиною кольору 24 біти, різного розміру.

У відкритих публікаціях запропонована дуже велика кількість різних стеганографічних методів, деякі з них є універсальними, інші призначені для широкого кола завдань. Найбільш поширені існуючі алгоритми використовують просторову область і область перетворення для приховування інформації. Для порівняльного оцінювання якості стеганографічних методів використовувалися загальновідомі показники, що дають кількісні та якісні оцінки.

Кількісні показники оперують із зображеннями на рівні пікселів і вважаються показниками візуальних спотворень стеганоконтейнера:

- співвідношення сигнал/шум:
$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}, \quad (1)$$

де $C_{x,\ y}$ – значення пікселя порожнього контейнера з координатами (x,y); $S_{x,\ y}$ – відповідне значення пікселя заповненого контейнера; *rows (C)* – кількість рядків у масиві C; *cols (C)* – кількість стовпців у масиві C;

- нормована середня абсолютна різниця:
$$NAD = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right|}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} \right|}, \quad (2)$$

- якість зображення:
$$IF = 1 - \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}, \quad (3)$$

- середньоквадратична похибка:
$$MSE = \frac{1}{X \cdot Y} \sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2, \quad (4)$$

- середня абсолютна різниця:
$$AD = \frac{1}{X \cdot Y} \sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right|. \quad (5)$$

До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, відносяться: пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування і вилучення. Вище вказані вимоги взаємно конкуруючі і не можуть бути оптимальними одночасно. Якщо необхідно приховати велике повідомлення всередині зображення, то неможливо вимагати абсолютної невидимості і високої стійкості. Завжди необхідний оптимальний компроміс (рис.1).

Рис.1. «Магічний трикутник» ключових характеристик стеганосистем

У роботі були розглянуті різні області застосування стеганографічних методів. Кожен з описаних додатків висуває різні вимоги до методу вбудовування даних. В той час, як окремі методи мають свої переваги та недоліки в реалізації та застосуванні для кожної області.

Таким чином, доцільною вважалася розробка комплексного критерію оцінювання стеганографічних систем, що на відміну від існуючих, буде враховувати вимоги до методів вбудовування в залежності від призначення системи з урахуванням важливості показників якості таких, як: пропускна здатність,

невидимість, захищеність, стійкість, складність вбудовування та вилучення прихованого повідомлення.

Другий розділ дисертації спрямовано на синтез комплексного критерію оцінювання стеганографічних систем. В ході виконання поставленого завдання здійснюється дослідження сучасних методів розрахунку коефіцієнтів важливості (КВ) та визначається найбільш доцільний для розрахунку КВ критеріїв оцінки стеганографічних систем, таких як пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення інформації. Визначається оптимальний за сукупністю критеріїв стеганографічний метод та характеристики, що потребують підвищення.

В роботі аналізуються основні підходи для розрахунку вагових коефіцієнтів, а саме: метод аналізу ієрархій (MAI), прямої розстановки ваг і ранжування факторів.

Залежність значень вагових коефіцієнтів від способу розрахунку та обробки експертних суджень показувався на даних, отриманих у процесі аналізу вимог до стеганографічних методів приховування даних при передачі мережами зв'язку. З робіт визнаних експертів зі стеганографії були визначені взаємні значення факторів вищезазначеними методами.

Зв'язок між ваговими коефіцієнтами, знайденими різними методами, оцінювався за допомогою коефіцієнта кореляції (КК):

$$r = \frac{n\sum xy - (\sum x \sum y)}{\sqrt{\left[n\sum x^2 - (\sum x)^2\right]\left[n\sum y^2 - (\sum y)^2\right]}}, \qquad (6)$$

де x, y – значення вагових коефіцієнтів, між якими оцінювався коефіцієнт кореляції.

Величина розходжень у різних експертів неоднакова і змінюється від 1% до 25%. Однак, як видно з рис. 2, тенденція корельованості результатів практично у всіх експертів однакова. Слід відзначити, що квазіпаралельний характер графіків кореляційних кривих дає підставу вважати логіку мислення експертів стійкою і підтверджує можливість використання результатів оцінок експертів у подальших дослідженнях.

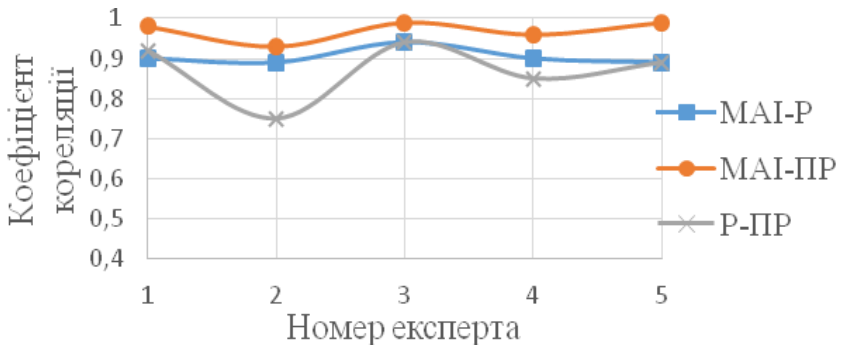


Рис. 2. Значення коефіцієнтів кореляції вагових коефіцієнтів за п'ятьма експертами

Проаналізувавши основні підходи до формування КВ найбільш придатними для подальшого визначення впливовості критеріїв та проведення порівняльної характеристики стеганографічних методів був обраний метод аналізу ієрархій.

Отже, сформулювавши вимоги сфер використання стеганографії до характеристик пропонується провести попарне порівняння показників методом аналізу ієрархій для кожного з додатків, використовуючи набір раніше запропонованих характеристик. Таким чином були побудовані матриці пріоритетів, що включають: пропускну здатність (*a*), стійкість (*b*), невидимість (*c*), захищеність (*d*), складність вбудовування (*e*) і складність вилучення (*f*). В табл. 1 наведений приклад для прихованого зв'язку.

Таблиця 1

Матриця пріоритетів (для додатку прихованого зв'язку)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		7	1	1	6	6
b	1/7		1/7	1/7	1/2	1/2
c	1	7		1	6	6
d	1	7	1		6	6
e	1/6	2	1/6	1/6		1
f	1/6	2	1/6	1/6	1	

Після побудови матриці пріоритетів, пріоритет кожного об'єкта в ієрархії визначається обчисленням відповідного елемента нормованого власного вектору матриці *V*.

Точне визначення основних пріоритетів власного вектора матриці є досить складним і може бути розраховано різними способами. В роботі був використаний спосіб, орієнтований на розрахунок середнього геометричного кожного рядка, згідно з яким компоненти вектора пріоритетів обчислюються таким чином:

$$V_i = \frac{\sqrt[N]{\prod_{j=1}^{N} W_{ij}}}{\sum_{k=1}^{N} \sqrt[N]{\prod_{j=1}^{N} W_{kj}}}, \qquad (7)$$

де N – розмірність пріоритетів; W_{ij} – елемент пріоритетів, що відображає результат порівняння елементів i і j.

Шляхом усереднення результатів для всіх додатків отримано ваги (важливість) кожної з характеристик стеганографічних алгоритмів (табл. 2).

Таблиця 2

Загальні ваги характеристик

Характеристика (*i*)	Вага (*R*)
Пропускна здатність	0,084
Стійкість	0,203
Невидимість	0,128
Захищеність	0,299
Складність вбудовування	0,070
Складність виявлення	0,218

Таким чином, результати оцінки показали, що найбільш важливими характеристиками стеганографічних методів є захищеність (вага R = 0,299), складність виявлення (вага R = 0,218) і стійкість (вага R = 0,203).

При наявності багатьох методів, досі не вирішена задача вибору оптимального метода за сукупністю критеріїв. Тож отримані оцінки використовувалися для аналізу обраних стеганографічних методів вбудовування інформації та для багатокритеріального вибору найкращого методу.

Порівняльний аналіз здійснювався на основі обраної методики попарних порівнянь окремо за кожною характеристикою. Результати порівняння стеганографічних методів за якісними критеріями оцінки приведені у табл. 3, де *A1* – метод заміни найменш значущих біт (НЗБ), *A2* – метод Куттера-Джордана-Боссена, *A3* – метод Коха-Жао, *A4* – метод Бенгама-Мемона-Ео-Юнга, *A5* – метод із розширенням спектру, *A6* – метод, засновані на 3-рівневому дискретному вейвлет-перетворенні (ДВП).

Дослідження показали, що при загальному оцінюванні методів, найкращі результати демонструє метод НЗБ (*A1, WW* = 0,266). Тоді як при більш детальному аналізі, враховуючи коефіцієнти важливості різних характеристик, найліпший результат показують методи, засновані на ДВП (*A6, WW1* = 0,333) та дискретному косинусному перетворенні (ДКП) (*A3, WW1* = 0,184).

Таблиця 3

Результати порівняння стеганографічних методів за якісними критеріями

Метод (*a*)	Значення (*WW*)	Значення (*WW1*)
A1	0,266	0,081
A2	0,181	0,086
A3	0,126	0,184
A4	0,097	0,146
A5	0,137	0,170
A6	0,193	0,333

Таким чином, на основі комплексного критерію, що враховує вимоги стеганографічних додатків, визначено оптимальні методи приховування інформації. Ефективність вживання ДКП і ДВП в стеганографічних методах пояснюється тим, що вони добре моделюють процес обробки зображення в ЗСЛ, відокремлюючи значимі деталі від другорядних. Таким чином, зазначені перетворення доцільніше використовувати в разі присутності активного порушника, оскільки модифікація значимих коефіцієнтів може привести до неприйнятного викривлення зображення.

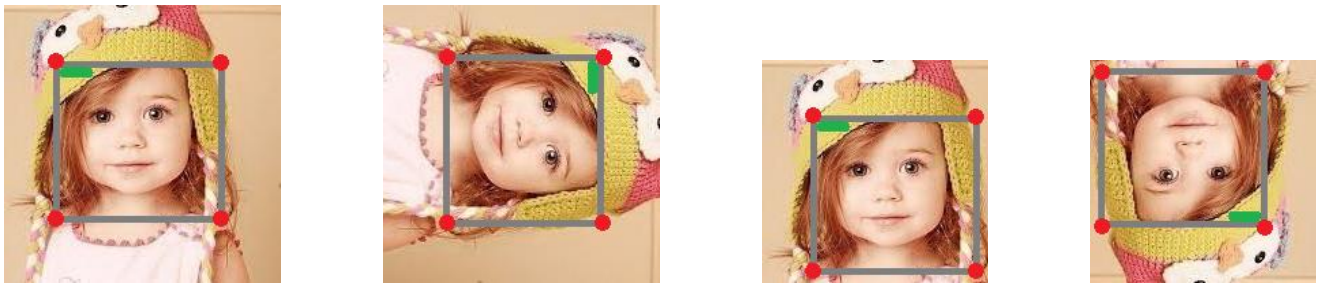
Також необхідно зазначити, що найвищі вимоги сфер використання стеганографії висуваються до стійкості, захищеності та складності вилучення вбудованого повідомлення. А в разі стеганографічної системи передачі інформації основним критерієм є забезпечення високої пропускної здатності.

У **третьому розділі** дисертаційної роботи досліджені методи протидії стеганографічних систем до завад та атак.

Здатність стеганографічних систем протидіяти атакам та завадам називається стійкістю або захищеністю, в залежності від умов та мети впливів. Стеганографічні додатки часто потерпають від завад у каналах звя'зку, наприклад, стеганосистеми прихованого зв'язку та системи захисту прав на зображення, та постійно піддаються атакам з боку користувачів, особливо при використанні стеганографіїї з метою відстеження порушника або виявлення випадків неліцензійного тиражування та шахрайства.

В ході досліджень було визначено, що найпоширенішими атаками на стеганографічні системи є геометричні атаки. Вони, на відміну від атак видалення, прагнуть змінити ЦВЗ шляхом внесення просторових або часових спотворень. Геометричні атаки математично моделюються як афінні перетворення з невідомим декодеру параметром. Ці атаки призводять до втрати синхронізації в детекторі ЦВЗ.

Однією із стратегій виявлення ЦВЗ після геометричних спотворень є спроба визначити, які перетворення були застосовані і інвертувати їх перед застосуванням стеганографічного детектора. Це може бути реалізоване за допомогою вбудовування реєстраційного шаблону разом із ЦВЗ (рис. 4) або надання ЦВЗ впізнаваної структури (рис. 5).



а *б* *в* *г*

Рис. 4. *а* – оригінальне зображення, *б* – зображення, повернуте на 90°, *в* – зображення, обрізане на 19% по горизонталі та на 18% по вертикалі , *г* – зображення, обрізане та повернуте на 180°

а *б* *в* *г* *д*

Рис. 5. *а* – оригінальне зображення із ЦВЗ, *б* – прогнозована автокореляційна функція, *в* – зображення із ЦВЗ, повернуте на 27° та зменшене до 91%, *г* – фільтрація зображення *в* нелінійним фільтром ВЧ, *д* – автокореляційна функція зображення із ЦВЗ

Ефективність даних методів досі була не досліджена, але достовірно відомо, що реалізація методу із наданням ЦВЗ впізнаваної структури істотно вплине на параметр складності вилучення прихованого повідомлення, що є не бажаним.

В свою чергу наявність завад у каналах зв'язку істотно впливає на можливість детектування та декодування вбудованого повідомлення. Методами боротьби з цією проблемою є дублювання міток початку та кінця повідомлення (рис.6), використання м'якого детектора та застосування завадостійкого кодування.

З підвищенням кількості міток спрацьовування детектора відбувається при менших значеннях співвідношення сигнал/шум (*Рс/Рш*). У порівнянні з жорстким детектуванням застосування м'якого детектування дозволяє у 1,7 рази зменшити співвідношення сигнал/шум, при якому спрацює детектор, та підвищити ймовірність вилучення прихованої інформації.

Використання трьох міток дозволяє підвищити ймовірність спрацювання жорсткого детектора на 28%, а м'якого – на 7%. Дублювання міток значно покращує роботу системи при використанні жорсткого детектора, а при використанні м'якого детектора є недоцільним, тому що не дає значного виграшу. Але використання м'якого детектування є більш ефективним, що надалі й буде використано при реалізації власного методу вбудовування.

Для підвищення ефективності роботи прихованої системи передачі інформації з м'яким детектуванням, на передавальній і приймальній стороні було реалізовано завадостійке кодування кодом Хемінга (12, 8). Подальші дослідження показали, що завадостійке кодування дозволяє зменшити ймовірність помилки в прийнятому повідомленні, а також підвищити ймовірність спрацювання детектора (рис. 7).

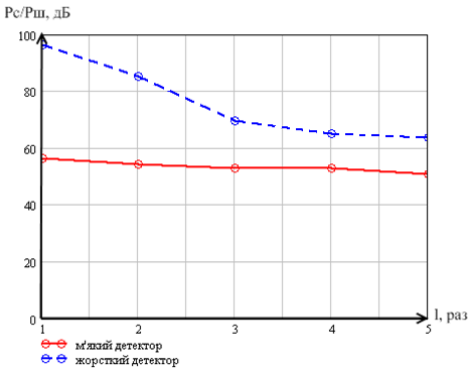


Рис. 6. Залежність мінімального значення *Рс/Рш* для спрацьовування м'якого та жорсткого детекторів при дублюванні міток

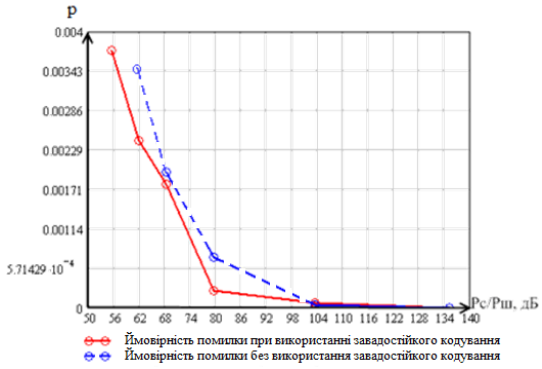


Рис. 7. Ймовірність помилки в використанні прийнятому повідомленні при завадостійкого кодування та без нього

Отже, застосування завадостійкого кодування дозволяє збільшити ймовірність безпомилкового прийому повідомлення до 66% при негативному впливі адитивного білого гаусового шуму в каналі зв'язку.

Використання запропонованих методів при побудові стеганографічних систем буде забезпечувати додаткову стійкість системи до можливих атак та захищеність при передачі по каналах зв'язку.

У **четвертому розділі** актуальним завданням було дослідження зміни параметрів зображення при зміні області вбудовування, оскільки незважаючи на їх широке поширення серед усіх ортогональних перетворень, в літературі відсутні рекомендації стосовно вибору типу вейвлету та області вбудовування.

Результат розрахунку нормованої середньої абсолютної різниці *NAD* для первинних областей перетворення LH та вторинних HL_2 та LH_2. відображено у вигляді діаграми на рис. 8.

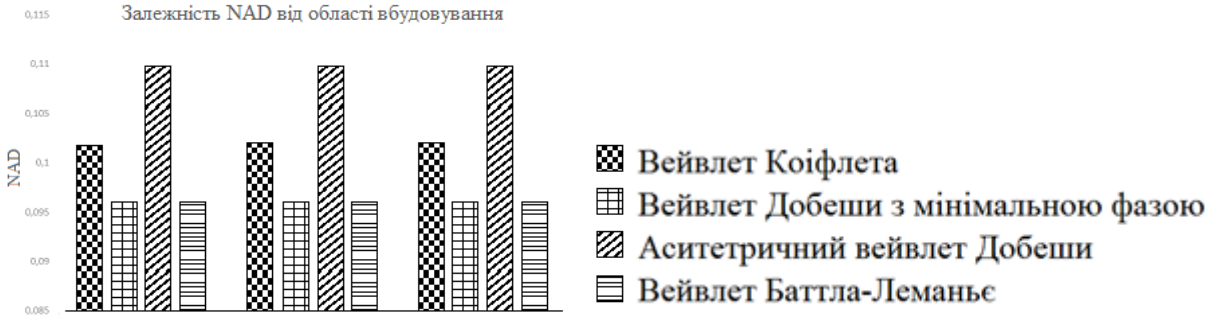
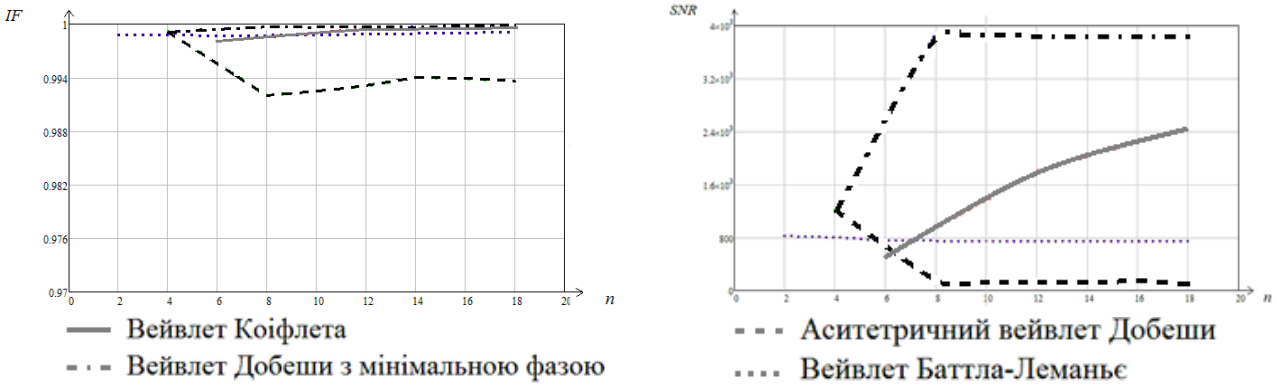


Рис. 8. Порівняння параметру *NAD* при використанні 1-ї (HL_2), 2-ї (LH) та 3-ї області (LH_2)

Вибір конкретного виду і типу вейвлета багато в чому залежить від сигналів, що аналізуються і завдань аналізу. В нашому випадку в якості критеріїв вибору вейвлет-функції будемо керуватися значеннями кількісних показників, що були обрані для проведення аналізу стеганографічних методів.

При проведенні досліджень аналізувалися стеганографічні системи, утворені із застосуванням вейвлета Койфлета, Бетла-Лємар'є, асиметричного вейвлета Добеші та вейвлета Добеші із мінімальною фазою. Результати для методу на основі дискретного вейвлет-перетворення (ДВП) на рис. 9 (а, б). Звідки можна нагально виділити вейвлет-функцію Добеши, що дозволяє досягти виграшів параметру *SNR* від 2-х до 5-ти разів. Отже, в подальших реалізаціях алгоритмів вбудовування доцільно використовувати саме цю функцію.



а *б*

Рис. 9. Порівняння параметрів (*а – IF*, *б – SNR*) для різних вейвлетів при зміні коефіцієнтів

Будь-яка система передачі інформації реалізується із прагненням до максимальної пропускної здатності. В роботі було запропоновано два методи

підвищення пропускної здатності при використанні методів вбудовування в область перетворення.

Перший максимально використовує середньочастотні компоненти зображення, а другий використовує для вбудовування не тільки синю матрицю зображення, як це прийнято, але й зелену. При цьому необхідно дотримуватись умови, щодо відсутності великих однотонних ділянок в зображенні-контейнері.

Спираючись на отримані результати, було вирішено надати подальшого розвитку існуючим методам на основі ДКП та ДВП. На рис. 10 представлені залежності кількісного параметру оцінки якості зображення *SNR* від умовної величини «біт вбудовування на блок зображення».

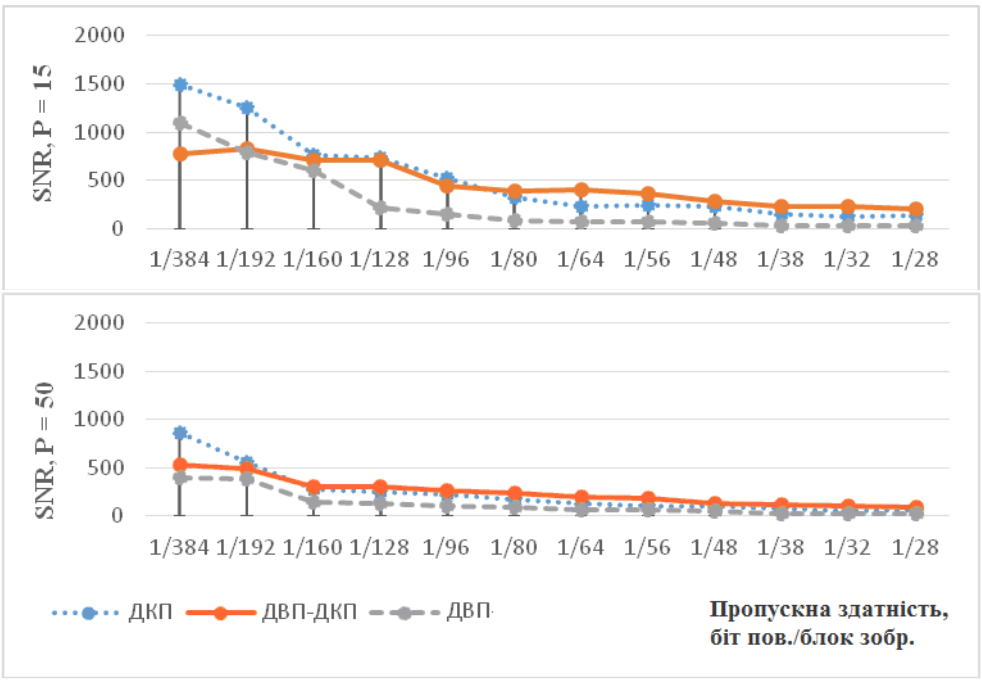


Рис. 10. Залежність *SNR* від кількості вбудованих біт на блок зображення

Всі дослідження проводилися для 3-х методів ДКП, ДВП та їх послідовного застосування. З графіків видно, що метод ДКП демонструє ліпші значення лише при вбудовуванні до 1-го біта повідомлення на 192 біти зображення. При збільшенні об’єму даних, доцільніше буде використовувати комбінований метод із ДВП та ДКП. При збільшенні потужності вбудовування ця залежність лише підсилюється.

Ще одним методом підвищення стійкості стеганографічної системи є збільшення порогової величини *P*, яка являє собою різницю між абсолютними значеннями коефіцієнтів ДКП, що і визначає біт вбудовування.

$$\begin{cases} \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| > P, при\ m_b = 0; \\ \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| < P, при\ m_b = 1, \end{cases} \quad (8)$$

де $\Omega_b(\upsilon, \nu)$ – матриці 8×8 коефіцієнтів ДКП, b – номер блоку контейнера C, (υ, ν) – позиція коефіцієнта в цьому блоці.

Чим більше значення *P*, тим стеганосистема, створена на основі даного методу, є стійкішою до компресії та впливу завад, проте якість зображення при цьому може значно погіршуватись. Тому ефективнішим буде використання методу, що дозволить максимально збільшити дану величину без істотних візуальних спотворень зображення (рис.11). На рис.11 зображені залежності для значення *SNR* від порогу вбудовування при різному об'ємі вкладень.

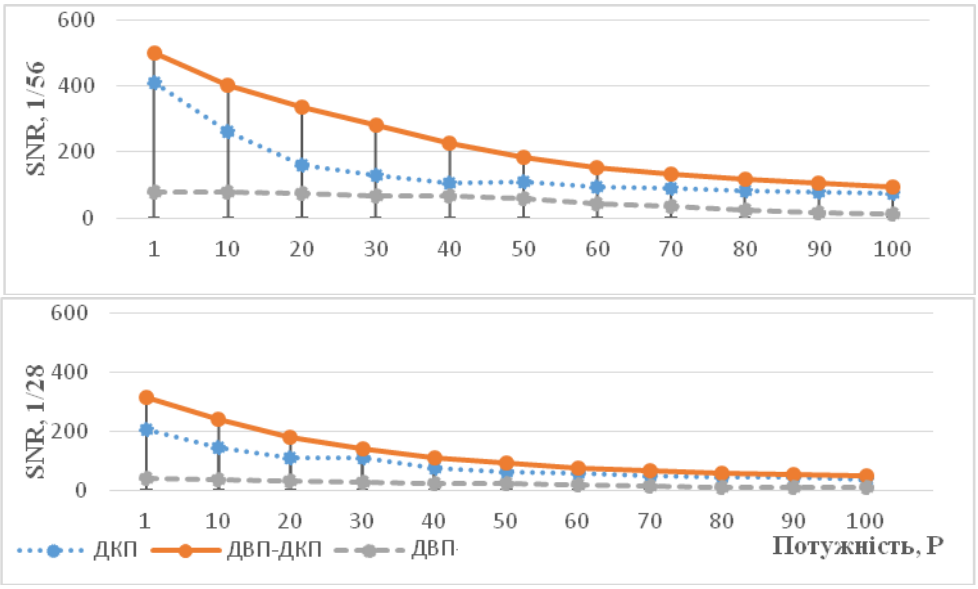


Рис. 11. Залежність *SNR* від потужності вбудовування (*а* – при вбудовуванні 1 біта на 56 пікселів зображення, *б* – при вбудовуванні 1 біта на 28 пікселів зображення

З графіків однозначно випливає, що найліпші характеристики демонструє метод на основі комбінованого використання ДВП та ДКП, що лягло в основу при розробці стеганографічного методу (рис.12).

Суть розробленого стеганографічного методу полягає в тому, що зображення та секретна інформація піддаються попередній обробці для підвищення загальної захищеності та стійкості стеганосистеми.

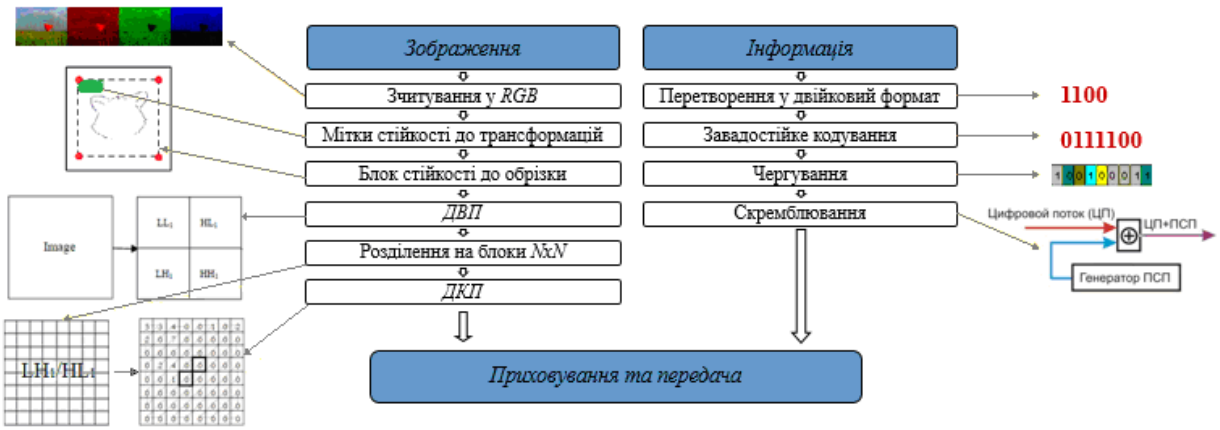


Рис. 12. Запропонована стеганографічна система приховування даних у цифрове зображення

Розроблений метод утворений шляхом інтеграції запропонованих методів підвищення стійкості, захищеності та пропускної здатності стеганографічних систем.

З метою демонстрації переваг розробленого методу було проведено порівняльний аналіз з обраними стеганографічними методами вбудовування інформації на основі методу попарних порівнянь із застосуванням комплексного критерію оцінювання (табл. 4). Найбільші значення є найліпшими.

Таблиця 4

Порівняння методів

Метод	Значення (*WW)*	Значення (*WW1)*
A1	0,248	0,188
A2	0,170	0,135
A3	0,084	0,094
A4	0,059	0,069
A5	0,090	0,084
A6	0,153	0,190
A7	0,196	0,241

Результати, що були отримані із нехтуванням важливості характеристик (*WW)*, знову ж таки показали найвищий коефіцієнт для методу НЗБ (*A1*). Тим не менш, з використанням оцінки ваг характеристик (*WW1)* провідну позицію займає запропонований синтезований метод (*A7*).

На підставі отриманих результатів багатокритеріальної оцінки можна впевнено стверджувати, що метод, заснований на послідовному застосуванні ДВП та ДКП (*A7*) показав найкращі властивості за стійкістю, невидимістю та захищеністю стеганографічної системи відносно інших найпоширеніших методів приховування інформації для передачі в мережі зв'язку.

Для порівняльного оцінювання якості стеганографічних методів також використовувалися загальновідомі показники, що дають кількісні оцінки (формула 1-5).

Методи були протестовані на зображеннях різних розмірів, а саме: *128x128*, *256x256*, *512x512*, *1024x1024*, *2048x2048* пікселів, з різною потужністю приховування для розробленого алгоритму: *P = 50, 30, 10, 5* (табл. 5).

Таблиця 5

Результати порівняння характеристик розробленого та існуючих методів

Показн. викривл	Оригінал	Розр. метод (*P*=50)	Розр. метод (*P*=30)	Розр. метод (*P*=15)	Розр. метод (*P*=5)
AD	0	0,649	0,539	0,456	0,406
SNR	∞	1675	3040	5983	6978
IF	1	≈1	≈1	≈1	≈1
MSE	0	2,113	1,04	0,566	0,422

Продовження табл. 5

Показн. Викривл	ДВП	Коха-Жао	Бенгама	Розшир. спектру	Куттера	НЗБ
AD	0,41	1,5	1,042	0,006	4,588	0,494
SNR	1237	997,42	1081,6	41480	192,2	4975
IF	≈1	0,995	0,998	≈1	0,995	≈1
MSE	0,45	9,4	10,2	0,006	235,7	0,404

Порівнюючи кількісні та якісні характеристики зроблено висновок, що розроблений метод є стійким до статистичного аналізу і не видає прихованого повідомлення суттєвими відхиленнями показників.

Значним досягненням є впровадження можливості детектувати і успішно здійснювати вилучення прихованого повідомлення, навіть при поворотах і обрізці зображення (табл. 6), що раніше унеможливлювало сам процес виявлення наявності прихованих вкладень.

Таблиця 6

Стійкість до атак

Вид геом. атаки	НЗБ	КДБ	КЖ	БМЕЮ	ДВП	Розр.мет.
1. Повороти	–	–	–	–	–	+
2. Відсічення	–	–	–	–	–	+
3. Яскравість	–	+	+	+	+	+
4. Контрастність	–	+	+	+	+	+

Доцільною вважалалася оцінка можливості розробленого методу адаптуватись до реальних каналів зв’язку та порівняти отримані значення з показниками, що демонструють існуючі методи. В результаті досліджень були отримані порогові значення спотворень, для яких ще можливе відновлення прихованої інформації (рис.13), та розраховані кількісні показники для оцінки методів.

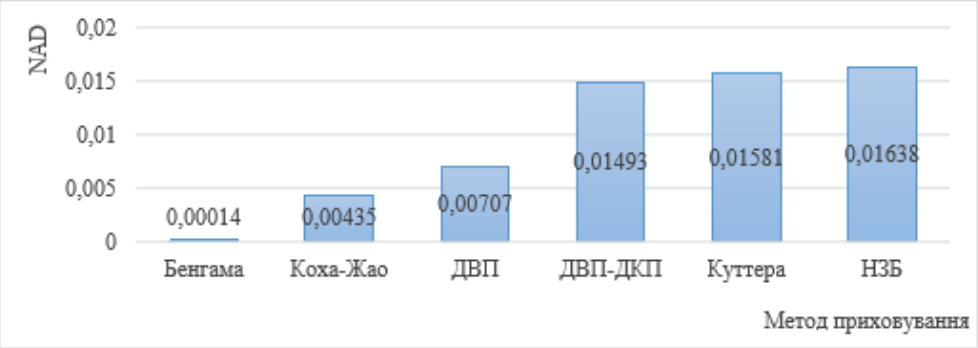


Рис. 13. Параметр *NAD* для порогових значень спотворень для кожного з методів

Порівнюючи порогові значення для синтезованого методу із раніше отриманими результатами, можна стверджувати, що він займає лідируючу позицію

серед методів, що використовують для вбудовування область перетворень. А також, демонструє показники, близькі до найкращих значень.

ВИСНОВКИ

У дисертаційній роботі вирішена актуальна науково-прикладна задача підвищення ефективності систем прихованої передачі інформації у телекомунікаційних системах на основі стеганографічного методу з високими показниками стійкості та пропускної здатності. Отримано кількісні значення багатокритеріального аналізу стеганографічних методів з використанням комплексного критерію оцінювання стеганографічних систем. Удосконалено стеганографічний метод вбудовування даних у вейвлет-коефіцієнти зображень. Удосконалено метод попередньої підготовки інформації до прихованої передачі телекомунікаційними системами. Удосконалено метод підвищення стійкості стеганографічних систем до геометричних атак. Розроблено стеганографічний метод вбудовування даних у нерухомі зображення, що забезпечує стійкість, захищеність, підвищує ймовірність правильного детектування вкладених даних та дозволяє збільшити пропускну здатність системи.

За результатами проведених теоретичних та експериментальних досліджень і розробок у дисертації досягнуті наступні наукові та практичні результати:

1) Визначено оптимальний метод багатокритеріальної оцінки для експертного оцінювання стеганографічних методів та характеристик, а саме метод аналізу ієрархій (MAI), що дозволяє оцінити адекватність оціночних суджень, і при отриманні квазіпаралельного характеру графіків кореляційних кривих дає підставу вважати логіку мислення експертів стійкою і підтверджує можливість використання результатів оцінок експертів у подальших дослідженнях.

2) Розроблено комплексний критерій оцінювання стеганографічних систем передачі інформації, який, на відміну від існуючих, враховує вимоги до методів вбудовування в залежності від призначення системи з урахуванням сукупності показників якості.

Було визначено, що найбільш важливими характеристиками стеганографічних методів в загальному випадку є захищеність (вага R = 0,299), складність виявлення (вага R = 0,218) та стійкість (вага R = 0,203). Це дає можливість сформулювати вимоги щодо покращення визначених характеристик задля підвищення загальної ефективності прихованої передачі інформації.

На основі комплексного критерію також були визначені оптимальні методи приховування інформації в разі присутності активного порушника. Найліпші результати показують методи, засновані на ДВП (*A6*, метрика *WW1* = 0,333) та ДКП (*A3*, метрика *WW1* = 0,184).

3) Вдосконалено стеганографічний метод вбудовування даних у вейвлет-коефіцієнти зображень шляхом інтеграції принципів частотного методу Коха-Жао,

розширення діагоналі вбудовування та використання двох матриць вейвлет-перетворення (HL та LH) для приховування повідомлення, що дає можливість підвищення пропускної здатності стеганографічної системи до 14 разів порівняно із класичними методами на основі вейвлет-перетворення.

4) Вдосконалено метод попередньої підготовки інформації до прихованої передачі телекомунікаційними системами, де застосування завадостійкого кодування дозволяє збільшити ймовірність безпомилкового прийому повідомлення до 66% при негативному впливі адитивного білого гаусового шуму в каналі зв'язку, а також метод адаптації телекомунікаційних систем передачі прихованої інформації до зовнішніх впливів, де застосування м'якого детектування дозволяє у 1,7 рази зменшити співвідношення сигнал/шум, при якому спрацює детектор, та підвищити ймовірність вилучення прихованої інформації.

5) Вдосконалено метод підвищення стійкості стеганографічних систем до геометричних атак, що відрізняється вбудовуванням реєстраційного шаблону разом із цифровим водяним знаком, дозволяє підвищити стійкість до атак проти стеганографічного детектора та збільшити ймовірність спрацьовування детектора на стороні отримувача при застосуванні атак на основі афінних перетворень, оскільки метод передбачує можливість обрізки зображення до N% та повороти на nπ/2 без втрати прихованих даних.

6) Розроблено новий стеганографічний метод вбудовування даних у нерухомі зображення на основі послідовного застосування дискретного косинусного та дискретного вейвлет-перетворення, який, на відміну від існуючих, демонструє вищі показники параметру *SNR* порівняно із методами на основі ДКП та методами на основі ДВП при вбудовуванні більше, ніж 1-го біта прихованого повідомлення на 192 біти зображення; дозволяє збільшити порогове значення *P* до 5 разів порівняно із методами на основі ДКП та методами на основі ДВП, що дозволяє підвищити стійкість стеганографічної системи до компресії та впливу завад без погіршення якості зображення; дозволяє підвищити ймовірність правильного прийому символу повідомлення в середньому на 55% та зменшити ймовірність групових помилок.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. *Вовк О.О.* Исследование стойкости методов скрытия информации в неподвижных изображениях / О.О. Вовк, А.А. Астраханцев, А.В. Дорожан // Системи обробки інформації (науково-технічний журнал). – Харків, 2012. – № 2 (54). – С. 104-109.

2. *Дорожан А.В.* Исследование характеристик методов скрытия на основе НЗБ на фоне аддитивного шума / А.В. Дорожан, А.А. Астраханцев, О.О. Вовк // Вісник національного технічного університету «ХПІ». – Харків, 2012. – №18. – С. 37 - 40.

3. *Вовк О.О.* Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів / О.О. Вовк, А.А. Астраханцев // Вісник національного

університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2014. – № 805. – С. 52 - 60.

4. *Астраханцев А.А.* Аналіз ефективності застосування вейвлет-перетворення в стеганографічних системах передавання даних / А.А. Астраханцев, О.О. Вовк // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2015. – № 832. – С. 9 - 17.

5. *Вовк О.О.* Синтез стеганографічного методу передачі даних, ефективного за критеріями надійності та захищеності / О.О. Вовк, А.А. Астраханцев // Електронне наукове фахове видання ХНУРЕ «Проблеми телекомунікацій». – Харків, 2015. – № 1 (16). – С. 103 - 115. – Режим доступу до журн.: http://pt.journal.kh.ua/2015/1/1/151_vovk_synthesis.pdf .

6. *Vovk O.* Synthesis of optimal steganographic method meeting given criteria / O. Vovk, A. Astrahantsev // Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska (technical and scientific journal). – Lublin, Poland, 2015. – P. 27 - 34.

7. Вовк О. О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / О. О. Вовк // Науковий журнал «Телекомунікаційні та інформаційні технології». – Київ, 2015. – №3. – С. 70 - 80.

8. *Вовк О.О.* Анализ атак на цифровые водяные знаки в видеофайлах и изображениях / О.О. Вовк наук. кер. А.А. Астраханцев // V Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя, ЗНТУ, 2010. – С. 88 - 90.

9. *Вовк О.О.* Дослідження стійкості та якості стеганографічних систем передачі інформації / О.О. Вовк, наук. кер. А.А. Астраханцев // Всеукраїнський конкурс студентських наукових робіт (галузь знань «Телекомунікаційні системи та мережі», «Інформаційні мережі зв'язку»). – Одеса, ОНАЗ, 2011р. – С. 4.

10. *Вовк О.О.* Дослідження стійкості цифрових водяних знаків у відеофайлах і зображеннях / О.О. Вовк, наук. кер. А.А. Астраханцев // 15-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». – Х.: ХНУРЭ, 2011. – т.4. – С. 157 - 158.

11. *Вовк О.О.* Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у мережах зв'язку / О.О. Вовк, наук. кер. А.А. Астраханцев // Інфокомунікації – сучасність та майбутнє: матеріали першої міжнародної науково-практичної конференції молодих вчених. – Одеса, ОНАЗ, 2011.– Ч.1. – С. 105 – 108.

12. *Вовк О.О.* Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у мережах зв'язку / О.О. Вовк, наук. кер. А.А. Астраханцев // Підсумкова науково-практична конференція Всеукраїнського конкурсу студентських наукових робіт (галузь знань «Інформаційна безпека»). – Львів, ЛП, 2012. – С. 4.

13. *Вовк О.О.* Сравнительный анализ устойчивости к атакам стеганографических методов скрытия информации / О.О. Вовк, А.А. Астраханцев // 9-я Международная молодёжная научно-техническая конференция «Современные проблемы радиотехники и телекоммуникаций РТ-2013». – Севастополь, 2013. – С. 153.

14. *Вовк О.О.* Определение уровня стойкости к атакам стеганографических методов скрытия информации / О.О. Вовк, А.А. Астраханцев // 23-я Международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии» (IEEE). – Севастополь, 2013. – С. 446 - 447.

15. *Вовк О.О.* Порівняльна характеристика методів стегоаналізу / О.О. Вовк, А.А. Астраханцев // Перша Міжнародна науково-практична конференція «Проблеми інфокомунікацій. Наука і технології». – Харків, 2013. – С. 57 - 58.

16. *Dorozhan A.* Synthesizing of an Improved Method for Hiding Data in Digital Images / O. Dorozhan, O. Vovk, A. Astrahantsev // «Modern problems of radio engineering, telecommunications, and computer science». – Lviv-Slavske, Ukraine, 2014. – P. 400 - 401.

17. *Vovk O.O.* The concept of steganographic algorithm which has high performance of characteristics defined as significant / O.O. Vovk, A.A. Astrahantsev // «Problems of Infocommunications. Science and Technology» (IEEE). – Kharkiv, Ukraine. 2014. – P. 177 - 179.

18. *Вовк О.О.* Концепція стеганографічного алгоритму стійкого до визначених критеріїв / О.О. Вовк, А.А. Астраханцев // Всеукраїнська науково-практична конференція «Сучасні проблеми телекомунікацій та підготовка фахівців у галузі телекомунікацій – 2014». – Л.: Львів, 2014. – С. 245-248.

19. *Бончук А.С.* Дослідження стійкості стеганографічних методів передачі інформації до стеганоаналізу / А.С. Бончук, наук. кер. О.О. Вовк // 19-й Міжнародний молодіжний форум «Радіоелектроніка і молодь у XXI столітті». – Х.: ХНУРЕ, 2015. – т.4. – С. 141 - 142.

20. *Vovk O.O.* New Steganographic Method: Development and Comparison with the Most Relevant / O.O. Vovk, A.A. Astrahantsev // «Problems of Infocommunications. Science and Technology» (IEEE). – Kharkiv, Ukraine. 2015. – P. 237 - 240.

21. *Семенко К.О.* Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / К.О. Семенко, наук. кер. О.О. Вовк // 20-й Міжнародний молодіжний форум «Радіоелектроніка і молодь у XXI столітті». – Х.: ХНУРЕ, 2016. – т.4. – С. 167 - 168.

АНОТАЦІЯ

Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Харківський національний університет радіоелектроніки, м. Харків, 2016.

Дисертаційну роботу присвячено розробці методу прихованої передачі інформації та цифрових водяних знаків, що є стійким до спотворень в каналах зв'язку та має високу пропускну здатність без втрат стійкості та рівня прихованості.

Проведено удосконалення стеганографічного метода вбудовування даних у вейвлет-коефіцієнти зображень. Для підвищення завадостійкості було запропоновано метод попередньої підготовки інформації до прихованої передачі, а також метод адаптації телекомунікаційних систем передачі прихованої інформації до зовнішніх впливів. В роботі запропоновано використання реєстраційного шаблону, вбудовування якого дозволяє підвищити загальну стійкість системи до атак на основі афінних перетворень.

На основі наведених вдосконалень при підготовці та приховуванні інформації, був розроблений метод вбудовування даних у нерухомі зображення, що дозволяє досягти основної мети роботи – підвищити стійкість вкладених даних та збільшити пропускну здатність системи прихованої передачі інформації.

Ключові слова: стеганографія, методи вбудовування даних у зображення, вейвлет перетворення, пропускна здатність, стійкість стеганосистем.

АННОТАЦИЯ

Вовк О.О. Методы повышения устойчивости и пропускной способности систем скрытой передачи информации. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – телекоммуникационные системы и сети. – Харьковский национальный университет радиоэлектроники, г. Харьков, 2016.

Диссертационная работа посвящена разработке метода передачи скрытой информации и цифровых водяных знаков, который является устойчивым к искажениям в каналах связи и имеет высокую пропускную способность без потерь устойчивости и уровня скрытности. В работе выполнен многокритериальный анализ стеганографических методов с использованием комплексного критерия оценки стеганографических систем, учитывающий требования к методам встраивания в зависимости от назначения стеганографической системы. По результатам оценки было определено множество методов для модернизации.

В ходе решения поставленной научной задачи в диссертационной работе получены следующие новые научные результаты. Впервые получены

количественные значения многокритериального анализа стеганографических методов с использованием комплексного критерия оценки стеганографических систем, которые в отличие от существующих, учитывают требования к методам встраивания в зависимости от назначения системы с учетом важности показателей качества. Было определено, что наиболее важными характеристиками стеганографических методов в общем случае являются защищенность (вес $R = 0{,}299$), сложность обнаружения (вес $R = 0{,}218$) и устойчивость (вес $R = 0{,}203$). Это дает возможность сформулировать требования по улучшению определенных характеристик для повышения общей эффективности скрытой передачи информации. На основе комплексного критерия также были определены оптимальные методы сокрытия информации в случае присутствия активного нарушителя. Лучшие результаты показывают методы, основанные на ДВП (*А6*, метрика *WW1* = 0,333) и ДКП (*А3*, метрика *WW1* = 0,184).

Усовершенствован стеганографический метод встраивания данных в вейвлет-коэффициенты изображений путем интеграции принципов частотного метода Коха-Жао, расширения диагонали встраивания и использования двух матриц вейвлет-преобразования (HL и LH) для сокрытия сообщения, что дает возможность повышения пропускной способности стеганографической системы до 14 раз по сравнению с классическими методами на основе вейвлет-преобразования.

Усовершенствован метод предварительной подготовки информации к скрытой передачи телекоммуникационными системами, где применение помехоустойчивого кодирования позволяет увеличить вероятность безошибочного приема сообщения до 66% при отрицательном воздействии аддитивного белого гауссова шума в канале связи, а также метод адаптации телекоммуникационных систем передачи скрытой информации к внешним воздействиям, где применение мягкого детектирования позволяет в 1,7 раза уменьшить соотношение сигнал/шум, при котором сработает детектор, и повысить вероятность извлечения скрытой информации.

Усовершенствован метод повышения устойчивости стеганографических систем к геометрическим атакам, отличающийся встраиванием регистрационного шаблона вместе с цифровым водяным знаком, что позволяет повысить устойчивость к атакам против стеганографического детектора и увеличить вероятность срабатывания детектора на стороне получателя при применении атак на основе аффинных преобразований, поскольку метод предусматривает возможность обрезки изображения до N% и повороты на $n\pi/2$ без потери скрытых данных.

На основе приведенных усовершенствований при подготовке и сокрытии информации был разработан новый стеганографический метод встраивания данных в неподвижные изображения, базирующийся на последовательном применении дискретного косинусного и дискретного вейвлет-преобразования, который, в отличие от существующих, демонстрирует высокие показатели параметра *SNR* по сравнению с методами на основе ДКП и методами на основе ДВП при встраивании больше, чем 1-го бита скрытого сообщения на 192 бита изображения; позволяет

увеличить пороговое значение *P* до 5 раз по сравнению с методами на основе ДКП и методами на основе ДВП; позволяет повысить устойчивость стеганографической системы к компрессии и воздействию помех без ухудшения качества изображения; позволяет повысить вероятность правильного приема символа сообщения в среднем на 55% и уменьшить вероятность групповых ошибок.

Ключевые слова: стеганография, методы встраивания данных в изображение, вейвлет-преобразование, пропускная способность, устойчивость стеганосистем.

ABSTRACT

Vovk O.O. Methods to improve the stability and capacity of covert communication systems. – Manuscript.

The dissertation on competition of an academic degree of Technical Sciences Candidate in the specialty 05.12.02 – telecommunication systems and network. – Kharkiv National University of Radio Electronics, Kharkiv, 2016.

The thesis is devoted to the development of the transmission method of hidden information and digital watermark that is resistant to distortions in communication channels and has high capacity without loss of stability and the level of secrecy.

The improvement of steganographic method of data embedding into the wavelet coefficients was done. The method of information preprocessing and method of telecommunication system adaptation were proposed to improve noise immunity during covert communication by the telecommunication systems. The paper presents usage of a registration pattern which can increase the overall stability of the system to attacks based on affine transformations.

Based on the improvements of preparing and concealing information was developed the method of embedding data into images, which allows to achieve the main goal of the work – to improve the stability of embedded data and increase capacity of covert communication systems.

Keywords: steganography, methods of embedding information into images, the wavelet transform, system capacity, steganosystem stability.

Формат 60х84/16. Ум. друк. арк. 0,9. Тир. 100 прим. Зам. 303-16
Підписано до друку 29.06.16. Папір офсетний.

Надруковано з макету замовника у ФОП Бровін О.В.
61022, м. Харків, вул. Трінклера, 2, корп.1, к.19. Т. (057) 758-01-08, (066) 822-71-30
Свідоцтво про внесення суб'єкта до Державного реєстру
видавців та виготовників видавничої продукції серія ДК 3587 від 23.09.09 р.