Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

На правах рукопису

ВОВК ОЛЕСЯ ОЛЕГІВНА

УДК 621.391

МЕТОДИ ПІДВИЩЕННЯ СТІЙКОСТІ ТА ПРОПУСКНОЇ ЗДАТНОСТІ СИСТЕМ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ

05.12.02 – Телекомунікаційні системи та мережі

Дисертація на здобуття наукового ступеня
кандидата технічних наук

Науковий керівник
Астраханцев Андрій Анатолійович
кандидат технічних наук, доцент

Харків – 2016

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD (Absolute Difference) – середня абсолютна різниця;

ASCII (American Standard Code for Information Interchange) – Американський стандартний код для інформаційного обміну;

BMP (Bitmap) – формат файлу зображень растрової графіки, в якому зображення зберігається у вигляді двовимірного масиву пікселів;

CMYK (Cyan, Magenta, Yellow, BlacK color) – субтрактивна колірна модель;

DVD (Digital Versatile Disc) – цифровий багатоцільовий диск;

GIF (Graphic Interchange Format) – формат обміну зображеннями;

ICO (Windows icon) – формат зберігання файлів значків;

IF (Image Fidelity) – якість зображення;

JPEG (Joint Photographic Expert Group) – растровий формат збереження графічної інформації, що використовує стиснення з втратами;

MSE (Mean Square Error) – середньоквадратична похибка;

NAD (Normalized Average Absolute Difference) – нормована середня абсолютна різниця;

PNG (Portable Network Graphic) – растровий формат збереження графічної інформації, що використовує стиснення без втрат;

RGB (Red, Green, Blue) – адитивна колірна модель, що описує спосіб синтезу кольору, за якою червоне, зелене та синє світло накладаються разом, змішуючись у різноманітні кольори;

SNR (Signal Noise Ratio) – співвідношення «сигнал/шум»;

TIFF (Tagged Image File Format) – один з базових універсальних форматів представлення високоякісних зображень;

YCbCr – сімейство колірних просторів;

АБГШ – адитивний білий гаусів шум;

БМЕЮ – метод Бенгама-Мемона-Ео-Юнга;

ВП – вейвлет-перетворення;

ВЧ – високочастотний;

ДВП – дискретне вейвлет-перетворення;

ДКЛП – дискретне перетворення Карунена-Лоєва;

ДКП – дискретне косинусне перетворення;

ДПФ – дискретне перетворення Фур'є;

ЗСЛ – зорова система людини;

КДБ – метод Кутера-Джордана-Боссена;

КЖ – метод Коха-Жао;

НВП – неперервне вейвлет-перетворення;

НЗБ – найменш значущий біт;

НЧ – низькочастотний;

ПЗЗ – прилад із зарядовим зв'язком;

ПСП – псевдовипадкова послідовність;

СЧ – середньочастотний;

ЦВЗ – цифровий водяний знак;

ЦОС – цифрова обробка сигналів.

ВСТУП

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 наукометричних базах Scopus та IEEE Xplore Digital Library.

РОЗДІЛ 1
ОГЛЯД ІСНУЮЧИХ РІШЕНЬ В ОБЛАСТІ ЦИФРОВОЇ СТЕГАНОГРАФІЇ

Стеганографія – це наука, яка вивчає способи та методи приховання конфіденційних даних. Її основною задачею є приховання саме факту існування таємних даних при передачі, зберіганні або обробці. Задача ж вилучення інформації відсувається на другий план і вирішується у більшості випадків стандартними криптографічними методами.

Інакше кажучи, під прихованням існування інформації мається на увазі не тільки неможливість виявлення у перехопленому повідомленні наявності іншого (прихованого) повідомлення, але і взагалі зробити неможливим виникнення будь-яких підозр із цього приводу, оскільки в останньому випадку проблема інформаційної безпеки повертається до стійкості криптографічного коду. Таким чином, займаючи своє місце у забезпеченні безпеки, стеганографія не замінює, а доповнює криптографію [22].

Стеганографія здійснюється у різні способи. Спільним в них є те, що приховане повідомлення вбудовується в деякий непримітний об’єкт, котрий потім відкрито пересилається адресату.

Історично напрямок стеганографічного приховання інформації був першим, але із часом у більшості був витіснений криптографією. Інтерес стеганографії відродився в останнє двадцятиріччя і був викликаний широким розповсюдженням технологій мультимедіа. Не менш важливим було виникнення нових типів каналів передачі інформації, що у сукупності із першим фактором дало новий імпульс розвитку і удосконаленню стеганографії, сприяло виникненню нових стеганографічних методів, в основу яких були покладені особливості представлення інформації у комп’ютерних файлах, обчислювальних мережах і т. і. Це, в свою чергу, дає можливість говорити про становлення нового напряму у сфері захисту інформації – комп’ютерної стеганографії [22].

На сьогоднішній день стеганографія є наукою, що швидко і динамічно розвивається, використовуючи при цьому методи і досягнення криптографії, цифрової обробки сигналів, теорії зв’язку і інформації.

Методи стеганографії дозволяють не тільки приховано передавати дані (так звана класична стеганографія), але й успішно вирішувати задачі завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження розповсюдження інформації мережами зв’язку, пошуку інформації у мультимедійних базах даних тощо. Ці обставини дозволяють у рамках традиційно існуючих інформаційних потоків або інформаційної середи вирішувати деякі важливі питання захисту інформації у ряді прикладних галузей.

Існують два основних напрями використання комп’ютерної стеганографії:

– ті, що поєднані із цифровою обробкою сигналів (ЦОС);

– ті, що не поєднані із ЦОС.

У першому випадку секретні повідомлення вбудовуються у цифрові дані, які, як правило, мають аналогову природу (мова, зображення, аудіо- і відеозаписи) [23].

У другому випадку – конфіденційна інформація розміщується у заголовках файлів або пакетів даних. Цей напрям не набув широкого використання із-за відносної легкості вилучення або знищення прихованої інформації.

Більшість поточних досліджень у сфері стеганографії так чи інакше пов’язані саме з ЦОС, що дозволяє говорити про цифрову стеганографію.

Можна виділити дві причини популярності досліджень у сфері стеганографії у наступний час: обмеження на використання крипто засобів у низці країн світу і поява проблеми захисту прав власності на інформацію, представлену у цифровому вигляді. Перша причина спричинила велику кількість досліджень у дусі класичної стеганографії (тобто приховання факту передачі інформації), друга – іще більш численні роботи у сфері так званих

водяних знаків. Цифровий водяний знак (ЦВЗ) – спеціальна мітка, що непомітно впроваджується у зображення або інший сигнал з метою тим чи іншим чином контролювати його використання [22].

Приховання інформації тільки на основі факту невідомості зловмиснику методу чи методів, закладених в основу приховання, на сьогоднішній день є малоефективним. Тому система безпеки повинна виконувати покладені на неї функції навіть при повній інформованості противника про її структуру і алгоритм функціонування.

1.1. Сфери застосування стеганографії

В даний час стеганографія може бути використана для прихованого зв'язку, захисту авторських прав на зображення (автентифікації), відбитків пальців (відстеження порушника), додавання заголовків до зображень, додавання додаткової інформації, такої як субтитри до відео, захисту цілісності зображень (виявлення випадків шахрайства), управління копіюванням при DVD записі та в інтелектуальних браузерах, для автоматичного надання інформації про авторські права, тощо.

Прикладом використання *прихованого зв'язку* може бути організація резервного каналу зв'язку, наприклад, з дипломатичними установами, що знаходяться на території іноземних держав. Стеганографія використовується для пересилки прихованих повідомлень у тоталітарних країнах, що вводять жорстку інтернет цензуру (рис. 1.1). В такому випадку необхідно враховувати, що місцеві канали зв'язку контролюються. Відправлення зашифрованих повідомлень неодмінно викличе підозру і може призвести до обмеження доступу до комунікаційної інфраструктури. Тому в інтересах відправника взагалі приховати присутність зв'язку. Ця ситуація може бути вирішена за допомогою підходящого стеганографічного протоколу [24].

Рис. 1.1. Блок-схема процесу вбудовування повідомлення при прихованому зв’язку

У звязку з бурхливим розвитком мультемидійних технологій гостро постало питання захисту *авторських прав* на зображення, тобто *автентифікації* (рис. 1.2). Прикладами можуть бути фотографії, аудіо і відеозаписи, тощо. Переваги, які дає представлення та передача інформації у цифровому вигляді, можуть бути перекреслені легкістю, з якою можлива їх крадіжка або модифікація. Наприклад, автор цифрового зображення хоче «підписати» зображення так, щоб було неможливо приписати авторство комусь іншому. Відомості автора не можуть бути додані до файла зображення, і не можуть бути помітно надруковані на зображенні, тому що такі підписи можуть бути легко видалені або замінені. Криптографічні цифрові підписи можуть бути застосовані лише для автентифікації каналу зв'язку, але не можуть захистити зображення, розміщене на веб-сторінці. Найліпшим способом захисту буде впровадження в зображення стійкого, захищеного, невидимого ЦВЗ. При цьому автор неодмінно зберігає оригінальне зображення. Для того, щоб довести своє авторство або навпаки розкрити підробку, автору необхідно перевірити наявність вбудованого ЦВЗ. Досвідчений крадій може спробувати видалити

оригінальний водяний знак або вставити свій підпис на зображення. Але це не принесе йому успіху, бо сліди обох ЦВЗ будуть присутні на зображенні, в той час, як автор може надати вихідний файл [24].

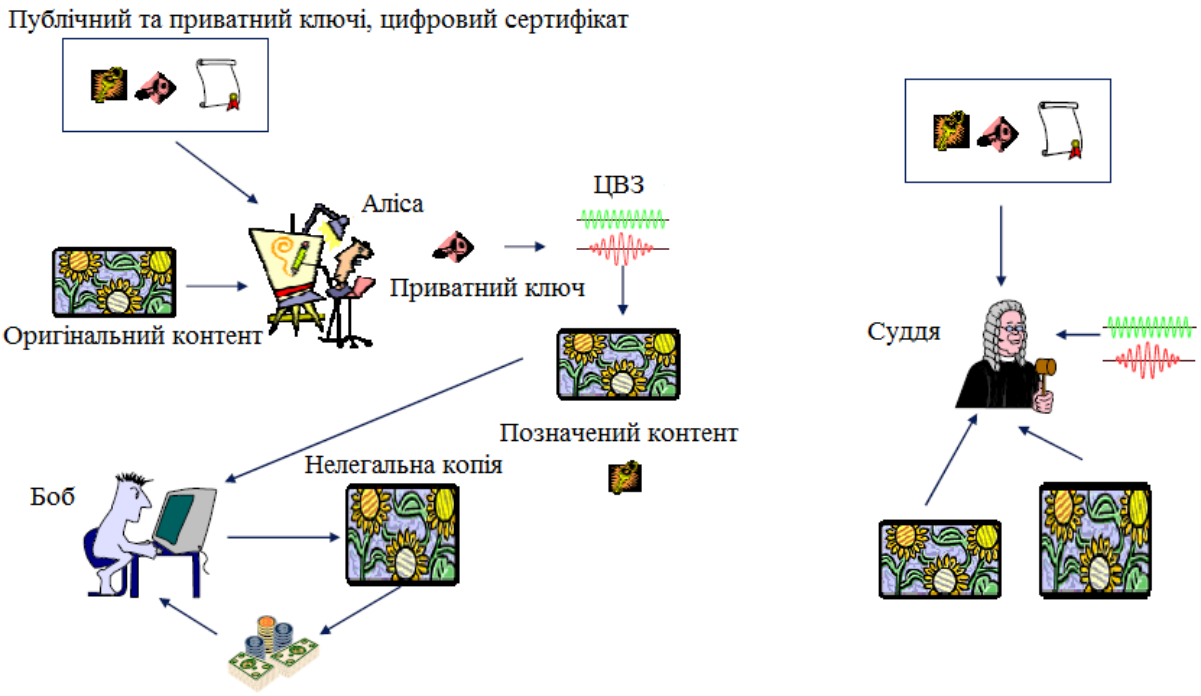


Рис. 1.2. Блок-схема процесу вбудовування ЦВЗ з метою захисту авторських прав

Технологія вбудовування *ідентифікаційних номерів* виробників має багато спільного з технологією ЦВЗ. Відмінність полягає в тому, що кожна захищена копія має свій унікальний номер вбудовування (звідси й назва – дослівно «*відбитки пальців*»). Цей ідентифікаційний номер дозволяє виробникові відстежувати подальшу долю свого продукту [22]. Широко розповсюдженим прикладом є продаж ліцензійних дисків. Завдяки унікальному номеру дуже легко визначити, хто саме робить і розповсюджує їх незаконні копії (рис. 1.3). Іншим сценарієм може бути поширення конфіденційної інформації (фото, відео) кільком депутатам і відстеження, хто є зрадником і через кого відбувається витік інформації ворогові. В цьому випадку неможливо використовувати видимий підпис, бо таке маркування буде виглядати підозріло

і може бути легко видалене. Розпізнавальні знаки повинні бути перцептивно невидимими і бути присутніми у кожному зображенні, що розповсюджується. Також, вбудовування має бути достатньо стійким, щоб не зруйнуватися при багаторазовому копіюванні та редагуванні.

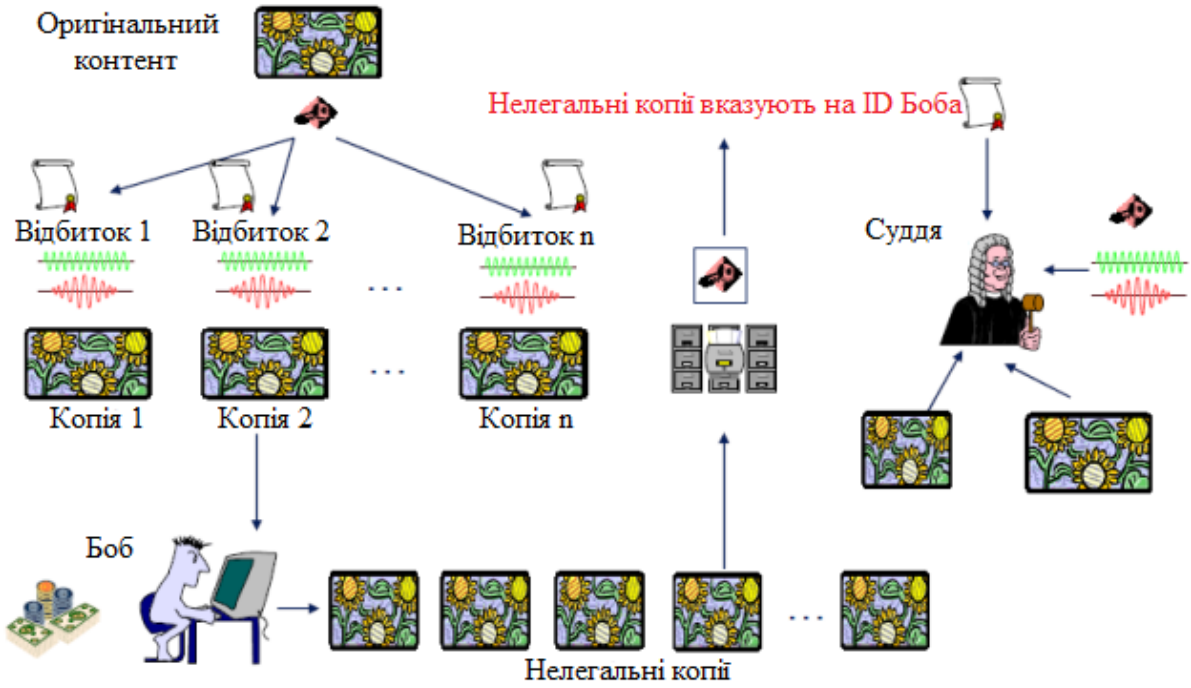


Рис. 1.3. Блок-схема процесу вбудовування ідентифікаційних номерів з метою відстеження порушника

Вбудовування заголовків може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту і т. і. Метою є зберігання різнорідно представленої інформації в одному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній потенційний порушник. Типовими прикладами є дубляж фільмів на декількох мовах, субтитри, відстеження використання даних (файл історії). Наприклад, одна копія фільму може розповсюджуватися з субтитрами на декількох мовах. Відеомагнітофон, DVD-програвач, телевізор та інші відео прилади можуть отримувати доступ і декодувати додатковий текст (субтитри) в режимі реального часу для кожного кадра, і відображати його на екрані телевізора. Хоча цей процес може бути

реалізовано скоріше шляхом додавання інформації, ніж непомітного вбудовування, однак вимоги до пропускної здатності та необхідність зміни формату інколи можуть не дозволити це зробити [24].

Однією із сфер застосування стеганографії є *захист цілісності зображення*, що дозволяє *виявляти випадки шахрайства* (рис. 1.4). Нажаль, на даний час цифрові зображення не можуть бути використані в суді в якості доказів через легкість виготовлення цифрових підробок та неможливість виявлення маніпуляцій із зображеннями. Вбудовування водяних знаків у цифрові зображення з метою виявлення місця і ступеня зміни зображення буде відігравати важливу роль у виявленні цифрового шахрайства, і може бути використане у суді. Перевага використання ЦВЗ очевидна: ЦВЗ не залежать від формату зображення, не збільшують пропускну здатність (на відміну від додавання заголовків), і не можуть бути видалені, щоб уникнути підробок. Пристрій формування зображення, такий як цифровий фотоапарат, відео-камера або сканер маркує зображення унікальним, стійким, захищеним водяним знаком, перш ніж вони будуть збережені на електронному носії або відправлені для відображення на інший пристрій, наприклад, комп'ютер [24].

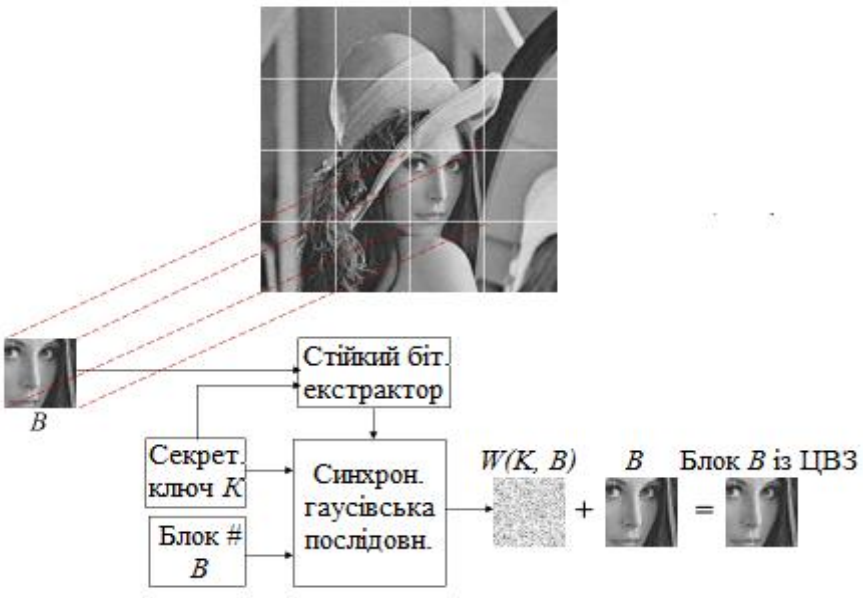


Рис. 1.4. Блок-схема процесу вбудовування ЦВЗ для захисту цілісності зображення

Широкою сферою застосування стеганографії є *управління копіюванням при DVD записі*. Комерційно поширювані фільми часто мають стійкий, невидимий водяний знак, який вказує чи можливе копіювання фільму [24]. DVD-програвач здатний отримувати доступ до водяного знаку та відмовитися від подальшого копіювання фільму на інший диск (рис. 1.5).

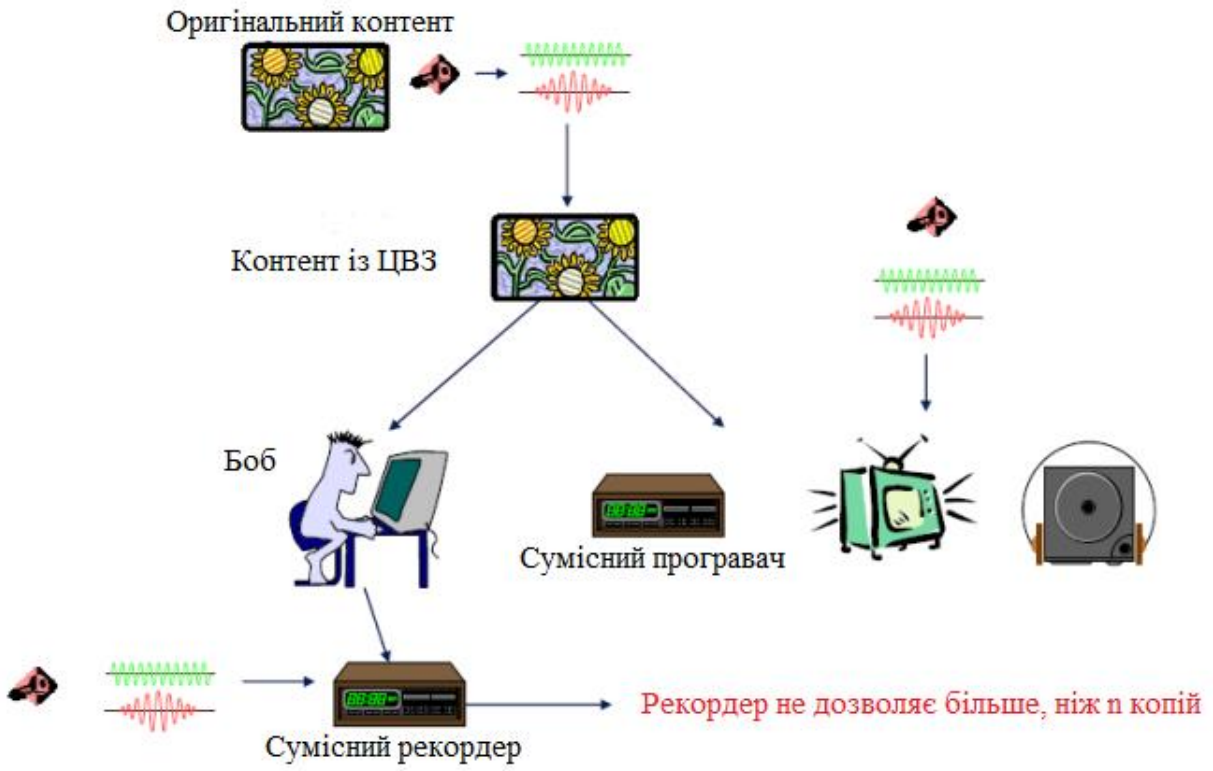


Рис. 1.5. Блок-схема процесу вбудовування ЦВЗ для управління копіюванням при записі DVD

Також методи стеганографії використовуються *в інтелектуальних браузерах та для автоматичного надання інформації про авторські права*. Після того, як зображення завантажилося, але до його відображення у браузері, воно перевіряється на наявність водяних знаків [24]. Якщо виявляються певні водяні знаки, то зображення не відображається, і автоматично стирається з пам'яті комп'ютера. Іншим застосуванням є відображення авторської інформації

кожного зображення, наданого браузером, програмного забезпечення, яким оброблювалося зображення, такими як PhotoShop або PaintShop і т. і.

1.2. Математична модель стеганосистеми як системи передачі інформації

Узагальнена структурна схема стеганосистеми як системи передачі інформації наведена на рис. 1.6 [25].

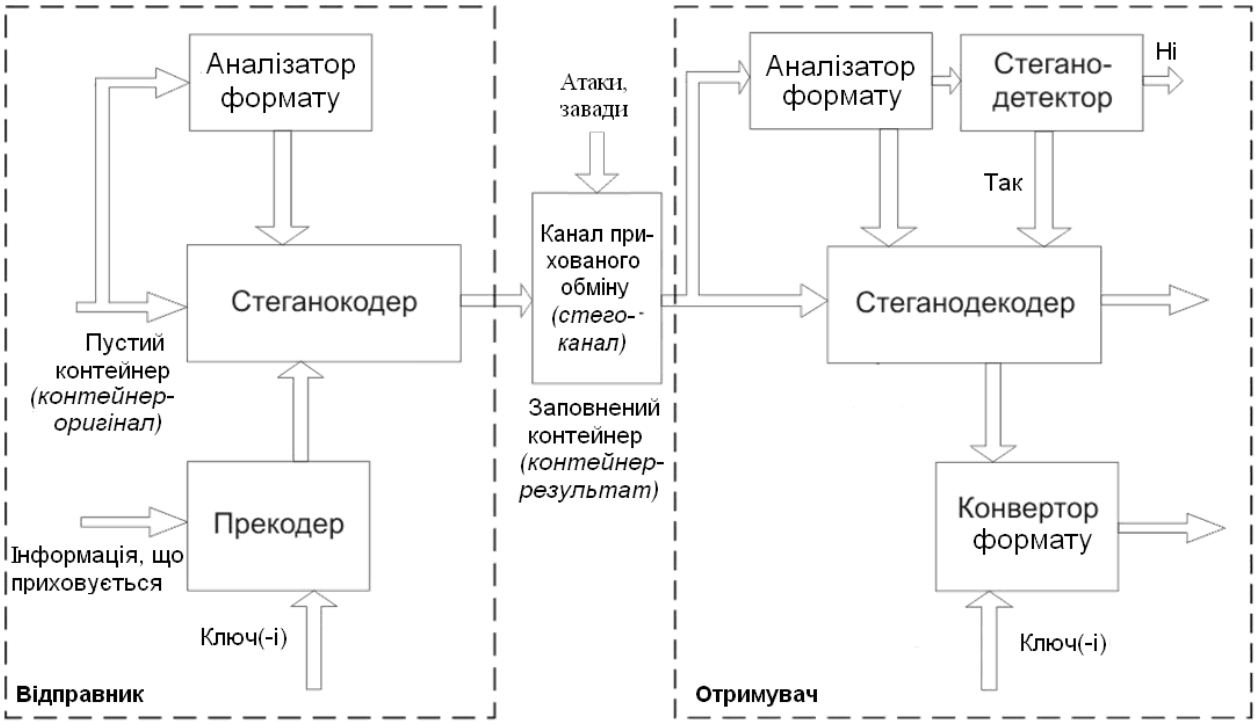


Рис. 1.6. Структурна схема стеганосистеми як системи передачі інформації

Передача файлу від відправника до отримувача починається з обробки секретної інформації, яку необхідно приховати, – *повідомлення*. Початкову обробку здійснює прекодер. Це необхідно для підвищення захищеності та стійкості стеганосистеми до спотворень. У більшості випадків при цьому використовується *ключ*, який зумовлює секретний алгоритм, що визначає порядок внесення повідомлення у *контейнер* [22].

Контейнером називається несекретна інформація, яку можна використовувати для приховання повідомлення. У якості повідомлення і контейнера можуть виступати як звичайний текст, так і файли мультимедійного формату.

Пустий контейнер (контейнер оригінал) – це контейнер, який не містить прихованої інформації.

Заповнений контейнер (контейнер результат) – контейнер, який вже містить приховану інформацію. Однією з важливих вимог, що при цьому ставиться є те, що контейнер-результат не повинен візуально відрізнятися від контейнера – оригіналу. Виділяють два основних типи контейнерів: потоковий і фіксований.

Потоковий контейнер являє собою послідовність бітів, що неперервно змінюється. Повідомлення вбудовується в неї у реальному масштабі часу, тому у кодері заздалегідь не відомо, чи вистачить розмірів контейнера для передачі всього повідомлення.

Основною ж проблемою є виконання синхронізації, визначення початку і кінця послідовності. Якщо у данній послідовності існують біти синхронізації, заголовки пакетів і т.ін., то прихована інформація може міститися одразу ж після них. Складність організації синхронізації є перевагою з точки зору забезпечення прихованості передачі.

У *фіксованому контейнері* розміри і характеристики контейнера заздалегідь відомі. Це дозволяє виконувати вкладення даних оптимальним чином. Тому надалі будемо говорити переважно про фіксований контейнер («контейнер»).

Контейнер може бути обраним, випадковим та нав’язаним. Обраний контейнер залежить від вбудованого повідомлення, а у крайньому випадку є його функцією. Такий тип контейнера найбільш характерний саме для стеганографії. Нав’язаний контейнер з’являється у випадку, коли той, хто надає контейнер, підозрює про ймовірність прихованої переписки і бажає запобігти їй. На практиці ж частіше за все мають справу із випадковими контейнерами.

Приховування інформації, яка переважно має великий об’єм, висуває істотні вимоги до контейнера, розмір якого повинен щонайменше у декілька разів перевищувати розмір даних, що вбудовуються. Зрозуміло, що для підвищення прихованості вказане співвідношення має бути якомого більшим.

Перед тим як виконати вкладення повідомлення у контейнер, йому необхідно надати певного зручного вигляду. Крім цього, перед упаковкою в контейнер, для підвищення захищеності секретної інформації останню можна зашифрувати стійким криптографічним кодом. У багатьох випадках також бажана стійкість отриманого стеганоповідомлення до викривлень (у тому числі і зловмисним).

У процесі передачі відео, зображення або будь-яка інша інформація, що використовується у якості контейнера, може зазнавати різних трансформацій (у тому числі з використанням алгоритмів із втратою даних): зміна об’єму, перетворення у інший формат тощо. Тому для збереження цілісності вбудованого повідомлення може знадобитися використання коду з виправленням помилок (завадостійке кодування).

Початкову обробку інформації, що приховується, виконує *прекодер*. У якості однієї з найважливіших попередніх обробок повідомлення (а також контейнера) можна назвати обчислення його узагальненого перетворення Фур’є. Що дозволяє здійснити вбудовування даних у спектральну область, що значно підвищує її стійкість до викривлень. Для підвищення секретності вбудовування попередня обробка часто виконується за допомогою ключа.

Пакування повідомлення у пустий контейнер, враховуючи формат контейнера, виконується за допомогою *стеганокодера*.

У більшості стеганосистем для пакування та вилучення повідомлень використовується *ключ*, який зумовлює секретний алгоритм, що визначає порядок внесення повідомлення в контейнер. Тип ключа обумовлює існування двох типів стеганосистем:

– із секретним ключем;

– із відкритим ключем.

У якості секретного алгоритму може використовуватися генератор псевдовипадкової послідовності (ПСП) бітів.

Прихована інформація заноситься у відповідності із ключем у ті біти, модифікація яких не призведе до істотних спотворень контейнера. Ці біти утворюють так званий стеганографічний канал.

Стеганографічний канал – це канал передачі контейнера-результата. Під час перебування у стеганографічному каналі контейнер, що містить приховане повідомлення, може піддаватися *навмисним атакам* або *випадковим завадам*.

У *стеганодетекторі*, враховуючи формат даних контейнера, визначається наявність у контейнері, можливо вже зміненому, прихованих даних. Ці зміни можуть бути обумовлені впливом помилок у каналі зв'язку, операцією обробки сигналу, навмисних атак порушників.

Розрізняють стеганодетектори, що призначені тільки для виявлення факту наявності вбудованого повідомлення, і пристрої, призначені для виділення цього повідомлення з контейнера, – *стеганодекодери* [22].

Отже, у стеганосистемі відбувається об'єднання двох типів інформації таким чином, щоб вони по різному сприймалися принципово різними детекторами. У якості одного з детекторів виступає система виділення прихованого повідомлення, в якості іншого – людина, що пред'являє до системи передачі вимоги, що досить важко формалізувати.

Для того, щоб стеганосистема була надійною і якісною, при її проектуванні необхідне виконання ряду вимог:

– Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення у візуально незначущі області сигналу. Однак, ці ж області використовують і алгоритми стиснення. Тому, якщо зображення буде надалі піддаватися стисненню, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися в візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів.

– Стеганосистема ЦВЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить. У деяких додатках таке виявлення може призвести до серйозних наслідків.

– Повинна забезпечуватися необхідна пропускна здатність.

– Стеганосистеми повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стеганокодер і простий стеганодекодер.

1.3. Критерії оцінки стеганосистем

Сьогодні запропонована дуже велика кількість різних стеганографічних методів, деякі з них є універсальними, інші призначені для широкого кола завдань. Для порівняльного оцінювання якості стеганографічних засобів можна використовувати загальновідомі показники, що дають кількісні та якісні оцінки.

1.3.1. Кількісні показники

Для порівняльного оцінювання ефективності стеганографічних засобів використовуються існуючі кількісні показники, які оперують із зображеннями на рівні пікселів, хоча після належної адаптації вони можуть бути застосовні й до інших способів опису зображення, а також до аудіо даних [25].

Найбільш популярним показником при аналізі рівня спотворень, які вносяться в контейнер під час приховання в ньому інформації, є взяте з радіотехніки співвідношення «сигнал/шум» (*SNR*). Воно є безрозмірною величиною, рівною відношенню корисного сигналу до шуму. Чим більше це відношення, тим менше шум спотворює зображення:

$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}, \quad (1.1)$$

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*), що показує ступінь відмінності між вихідним контейнером і контейнером з вбудованим секретним файлом, розраховується в такий спосіб:

$$NAD = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right|}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} \right|}. \quad (1.2)$$

Якість зображення (*IF*) є однією з основних оціночих характеристик для стеганографічних методів, які працюють із зображеннями. Тому що візуальна атака заснована на здатності зорової системи людини аналізувати зорові образи й виявляти істотні розходження в зображеннях. Вона характеризує ступінь відповідності порожнього контейнера до заповненого:

$$IF = 1 - \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}. \quad (1.3)$$

Середньоквадратична похибка (*MSE*) є середньоквадратичним відхиленням вибіркового розподілу статистичних даних. Тобто, її можна використовувати для оцінки точності вибіркового середнього значення:

$$MSE = \frac{1}{X \cdot Y} \sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2 . \quad (1.4)$$

Середня абсолютна різниця (*AD*), що визначає середнє значення модулю різниці між пікселями порожнього і заповненого контейнеру. Велике значення *AD* вказує на низьку якість зображення:

$$AD = \frac{1}{X \cdot Y} \sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right| . \quad (1.5)$$

1.3.2. Якісні показники

До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, відносяться:

Пропускна здатність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру. Стеганосистема повинна забезпечувати необхідну пропускну здатність [24].

Стійкість – здатність вилучити приховану інформацію після загальних операцій з обробки зображень: лінійні і нелінійні фільтри (розмитість, підвищення різкості, медіанна фільтрація), стиснення з втратами, регулювання контрастності, перефарбування, передискретизації, масштабування, обертання, додавання шуму, обрізки, друку/копіювання/сканування, перестановки пікселів у вузькій околиці [26], квантування кольорів тощо. Наголошуємо, що поняття стійкості не включає атаки на метод вбудовування, які ґрунтуються на знанні алгоритму приховування або вилучення. Стійкість означає, стійкість до «сліпих», нецільових модифікацій, або загальних операцій з зображеннями.

Невидимість – характеристика, що відповідає за неспроможність людського зору виявити стеганографічне повідомлення без використання

спеціальних засобів. Це поняття спирається суто на властивості зорової системи людини (ЗСЛ). Прихована інформація вважається непомітною, якщо середньостатистична людина не здатна відрізнити носій з прихованою інформацією від носія без неї. Загальноприйнята схема експерименту (так званий сліпий тест), що часто використовується в психо-візуальних експериментах, засновується на тому, що суб'єктам пропонується в довільному порядку велика кількість носіїв із вбудованою інформацією і без, та пропонується обрати, які саме носії містять приховані дані [24].

Відзначимо, що поняття невидимості може бути визначене й іншим способом та бути пов'язаним із статистичною моделлю джерела зображення. Тоді вважається, що прихована інформація є невидимою, якщо заповнене зображення-контейнер узгоджується з моделлю джерела, звідки було взяте вихідне зображення, і може бути розраховане об'єктивним шляхом, наприклад, за допомогою показника *IF*.

Захищеність – вбудована інформація не може бути видалена цілеспрямованими атаками, заснованими на відомому алгоритмі вбудовування та вилучення (окрім секретного ключа), і знанні принаймні одного носія з прихованим повідомленням. Поняття захищеності також включає в себе процедурні атаки, такі як атаки IBM [27] або атаки на основі знання про часткову модифікацію носія через наявність вкладення [28].

Складність вбудовування і вилучення – кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення. Стеганосистеми повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізація стеганографічної системи передачі інформації, тобто складний стеганокодер і простий стеганодекодер.

Вищевказані 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. З іншого боку, якщо

потребується стійкість до великих спотворень, то повідомлення, що має бути надійно сховане, не може бути занадто довгим. Це спостереження схематично зображене на рис. 1.7.

Рис. 1.7. «Магічний трикутник» ключових характеристик стеганосистем

1.4. Обґрунтування вибору зображення для вбудовування

На сьогоднішній день існує велика кількість методів приховування даних саме у цифрових зображеннях. Це обумовлено наступними причинами [22]:

– існування практично значимої потреби захисту фотографій, картин від незаконного тиражування й поширення;

– великий обсяг цифрового подання зображень, що дозволяє впроваджувати ЦВЗ великого об’єму або підвищувати стійкість впровадження;

– заздалегідь відомий розмір контейнера, відсутність обмежень, що накладаються вимогами реального часу;

– наявність в більшості реальних зображень текстурних областей, що мають шумову структуру й добре підходять для вбудовування інформації;

– слабка чутливість людського ока до незначних змін кольорів зображення, його яскравості, контрастності, рівня шуму в ньому, перекручування поблизу контурів;

– добре розроблені методи цифрової обробки зображень.

Однак, остання причина викликає й значні труднощі у забезпеченні стійкості ЦВЗ: чим сучаснішими стають методи компресії, тим менше залишається можливостей для вбудовування сторонньої інформації [28].

Абсолютно зрозумілою є необхідність прийняття до уваги стеганометодами не тільки алгоритмів компресії зображень, але й властивостей ЗСЛ.

Властивості ЗСЛ можна розділити на дві групи: низькорівневі («фізіологічні») і високорівневі («психофізіологічні») [22].

Виділяють три найважливіших низькорівневих властивості, що впливають на помітність стороннього шуму в зображенні:

– чутливість до зміни яскравості (контрастності) зображення;

– частотна чутливість;

– ефект маскування.

На рис. 1.8 зображена залежність мінімального контрасту ΔI/I від яскравості.

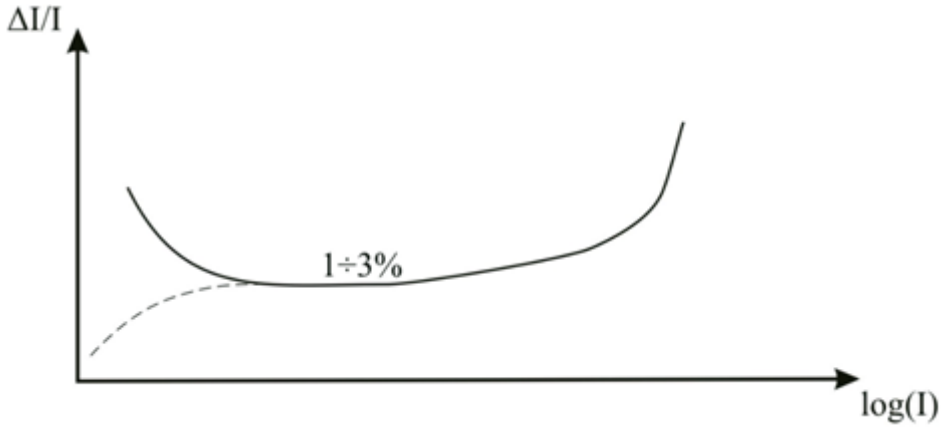


Рис. 1.8. Чутливість до зміни контрасту і поріг непомітності ΔI

Як видно, для середнього діапазону зміни яскравості контраст приблизно постійний, тоді як для малих і великих яскравостей значення порога непомітності (ΔI) зростає. Встановлено, що $\Delta I \approx (0.01 \div 0.03) \cdot I$ для середніх значень яскравості.

Крім того, у [22] зазначено, що результати новітніх досліджень суперечать «класичній» теорії і показують, що при малих значеннях яскравості поріг непомітності зменшується, тобто ЗСЛ більш чутлива до шуму в цьому діапазоні.

Частотна чутливість ЗСЛ проявляється у тому, що людина набагато більш сприйнятлива до низькочастотного (НЧ), ніж до високочастотного (ВЧ) шуму. Це пов'язано з нерівномірністю амплітудно-частотної характеристики ЗСЛ.

Елементи ЗСЛ поділяють сигнал, що надходить, на окремі складові, кожна з яких збуджує нервові закінчення очей через ряд підканалів. Складові, що виділяються оком, мають різні просторові і частотні характеристики, а також різну просторову орієнтацію (горизонтальну, вертикальну, діагональну) [30].

У разі одночасного впливу на око двох складових зі схожими характеристиками збуджуються одні й ті ж підканали. Це призводить до ефекту маскування, який полягає у збільшенні порога виявлення зорового сигналу в присутності іншого сигналу, що має аналогічні характеристики. Тому, адитивний шум набагато помітніший на НЧ (однотонних) ділянках зображення в порівнянні з ВЧ ділянками, тобто, в останньому випадку спостерігається маскування. Найбільш сильно даний ефект проявляється, коли обидва сигнали мають однакову орієнтацію і місце розташування [22].

Частотна чутливість тісно пов'язана з яскравістю. Відомо також і вираз для визначення порогу маскування на основі відомої яскравісної чутливості, що дозволяє знайти метрику спотворення зображення, яка враховувала б властивості ЗСЛ. Математичні моделі такого типу добре розроблені для випадку квантування коефіцієнтів ДКП, оскільки саме воно застосовується в стандарті *JPEG*.

Високорівневі властивості ЗСЛ відрізняються від низькорівневих тим, що проявляються «вторинно» – обробивши первинну інформацію від ЗСЛ, мозок видає команди на «підстроювання» зорової системи під зображення.

Перелічимо основні з цих властивостей:

– чутливість до контрасту – висококонтрастні ділянки зображення і перепади яскравості звертають на себе більше уваги;

– чутливість до розміру – великі ділянки зображення більш «помітні» у порівнянні з меншими за розміром, причому існує поріг насиченості, коли подальше збільшення розміру не грає ролі;

– чутливість до форми – довгі і тонкі об'єкти викликають більше уваги, ніж закруглені і однорідні;

– чутливість до кольорів – деякі кольори (наприклад, червоний) більш «помітні», ніж інші (рис. 1.9); цей ефект посилюється, якщо фон заднього плану відрізняється від кольорів фігур на ньому;

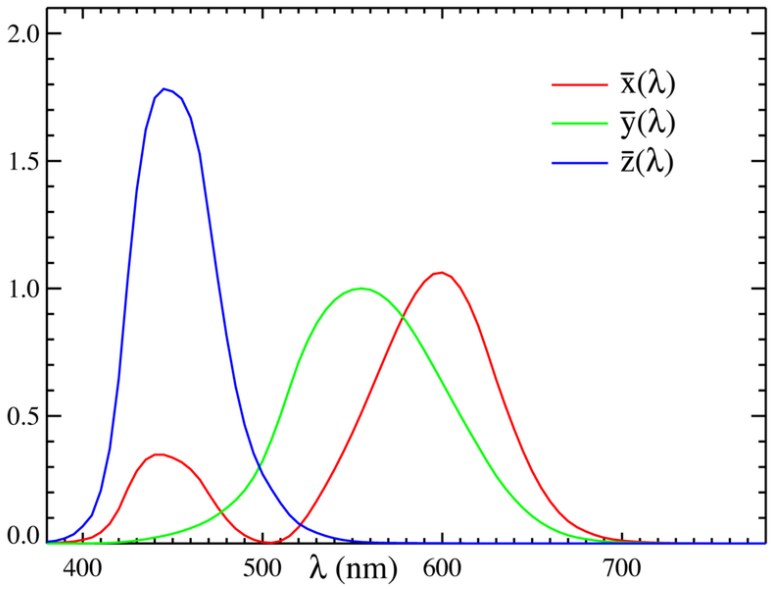


Рис. 1.9. Функції колірної відповідності Стандартного колориметричного спостерігача

– чутливість до місця розміщення – людина схильна в першу чергу розглядати центр зображення; також уважніше розглядаються фігури переднього плану, ніж заднього;

– чутливість до зовнішніх подразників – рух очей спостерігачів залежить від конкретної обстановки, від отриманих ними перед переглядом або під час його інструкцій, додаткової інформації.

Дотримуючись рекомендацій по роботі ЗСЛ, можна запобігти виявленню прихованих даних методом візуальної атаки. Бо саме вона заснована на здатності ЗСЛ аналізувати зорові образи й виявляти істотні розходження в зображеннях.

1.4.1 Типи цифрових зображень

В сучасному процесі поліграфічного виробництва всі ілюстрації й елементи оформлення представлені цифровими зображеннями різних типів. Цифрові зображення за способом дискретизації оригіналу поділяються на растрові, векторні та змішаного типу.

До *растрових зображень* відносяться двомірні масиви даних (матриці пікселів), кожен елемент яких представляє ділянку оригіналу з усередненим колірним показником [31].

Растрові зображення отримують двома способами. Перший – сканування оригіналу – проводиться за допомогою особливого пристрою – сканера, в якому кожен оптичний елемент ПЗЗ-лінійки (або ПЗЗ-матриці) зчитує яскравості і колірні характеристики оригіналу. Ці характеристики перетворюються в двійковий код кольору і посилаються в осередку двомірного масиву даних (матриці пікселів). Другий спосіб отримання растрового зображення – проектування оригіналу на ПЗЗ-матрицю через систему лінз (об'єктив). Цей спосіб растрового аналого-цифрового перетворення характерний для цифрових фотоапаратів і відеокамер.

Основні характеристики растрового зображення – розмір та глибина кольору.

Розмір зображення в пікселях – це кількість рядків і стовпців матриці, що використовуються для зберігання зображення. Розмір цифрового зображення можна довільно змінювати, змінюючи фізичний розмір картинки при друку, при цьому розмір матриці пікселів буде залишатися незмінним.

Глибина кольору – це характеристика, яка визначає якість відтворення кольору, кількість відтінків, які можуть відображати елементи матриці пікселів.

Кожен елемент масиву даних (матриці) являє собою число в двійковій системі числення. Його розмірність визначається в бітах. Глибина кольору – це кількість біт на піксель зображення. За допомогою одного байта (8 біт) можна задати 256 кольорів (як правило чорно-білих). Колір пікселя задається як поєднання трьох кольорів (червоного, зеленого, блакитного) у різних відношшеннях (рис. 1.10).

R	G	B	Колір
0	0	0	чорний
0	0	1	майже чорний
255	0	0	червоний
0	255	0	зелений
0	0	255	синій
128	128	128	сірий
255	255	255	білий

Рис. 1.10. Приклади представлення кольорів пікселя через три кольорових компоненти

При аналого-цифровому перетворенні завжди відбувається втрата деякої кількості інформації, оскільки дискретизація завжди проводиться шляхом усереднення та узагальнення потоку вихідної аналогової інформації. Звідси

основний недолік растрових цифрових зображень – неможливість їх масштабування без втрати якості.

Основна сфера застосування растрових зображень – це фотографічні ілюстрації. Растрові зображення використовуються у всіх випадках, коли необхідно відтворити аналоговий оригінал, будь то фотографія, малюнок, складний елемент оформлення, який нераціонально переводити в вектори.

Іншим видом цифрових зображень є *векторні зображення*. Найменшими елементами векторного зображення є вектор і крива Безьє. Основним керуючим елементом кривої Безьє є вузол, що також називається контрольною точкою або контрольною вершиною. Ступінь кривизни лінії визначаються координатами вузла і двох керуючих точок [31].

Контур зображення в цифровому вигляді являє собою масив даних, що містить координати контрольних та керуючих точок, а також характеристики кривої в цілому – її товщину, колір, напрямок, а якщо крива замкнута – то і колір і тип заливки.

Векторні зображення отримують двома способами – шляхом ручного трасування оригіналу і шляхом автоматичного трасування.

Основна перевага векторного зображення – це можливість масштабування без втрати якості. Ще одним плюсом векторних зображень є порівняно невеликий розмір файлів, що їх містять. Це робить зручною передачу векторних зображень по електронних каналах зв'язку.

Головний недолік векторних зображень – це те, що вони майже завжди відтворюють оригінал в спрощеному вигляді (рис. 1.11). Деякі деталі оригіналу буває неможливо відтворити у векторному зображенні.

Рідко векторні зображення є повноцінними ілюстраціями.

а *б*

Рис. 1.11. Приклад растрового (*а*) та векторного (*б*) зображень

Цифрові зображення *змішаного типу* являють собою масиви даних, що містять інформацію як у вигляді матриці пікселів, так і у вигляді опису векторів, кривих Безьє, примітивів і текстових блоків [31].

В основі вертикальної структури векторно-растрових зображень лежить поняття шару. Шар – це область даних, що містить інформацію про окремий елемент вертикальної структури зображення.

Векторно-растрові зображення отримують з вихідних векторних і растрових елементів шляхом зведення за допомогою графічних редакторів. Також умовно до зображень змішаного типу слід віднести результати роботи програм комп'ютерної верстки, в яких якості основного векторного елемента виступають текстові блоки.

Зображення змішаного типу поєднують в собі переваги й недоліки тих типів зображень, які присутні в них у вигляді елементів (шарів).

Основною перевагою зображень змішаного типу є можливість вільного редагування кожного шару окремо, а основним недоліком – великий обсяг масиву даних і, відповідно, кінцевого файлу.

Отже, не зважаючи на деякі недоліки растрових зображень, вони наразі є найпоширенішими у використанні – растрова графіка використовується практично скрізь: від маленьких значків до плакатів. Вона дозволяє створити практично будь-яке зображення, незалежно від складності, на відміну від векторної, де неможливо точно передати ефект переходу від одного кольору до іншого без втрат у розмірі файлу.

1.4.2. Огляд форматів зберігання зображень

Растрові зображення зазвичай зберігаються в стислому вигляді. Залежно від типу стиснення може бути можливо або неможливо відновити зображення в точності таким, яким воно було до стиснення (стиснення без втрат або стиснення з втратами відповідно). Так само в графічному файлі може зберігатися додаткова інформація: про автора файлу, фотокамери і її налаштуваннях, кількості точок на дюйм при друці та ін.

У сучасній машинній графіці використовуються десятки спеціалізованих форматів даних. Деякі з них розроблені окремими фірмами під конкретні програмні засоби, інші створені науково-дослідними установами, у більшій чи меншій мірі пов'язаними співпрацею з Міжнародною організацією стандартів (iso.org). Проте у повсякденній практиці зустрічається всього лише декілька [31].

Найпростіший формат – *BMP* (BitMaP, тобто бітова карта), який з'явився з першими версіями операційної системи Microsoft Windows. Він громіздкий, але дозволяє повністю і без втрат створювати копію файлу, при максимальній якості. Аналогічним є формат *ico* для зображення у системі Windows так званих іконок – мініатюрних значків-логотипів програм.

Іншим растровим форматом є *TIFF* (Tagged Image File Format), тобто структурований формат файлу зображення, і саме йому віддають перевагу професіонали. Він був розроблений досить давно, зазнав доповнень, модифікацій та вдосконалень, має велику кількість спеціалізованих варіантів та

версій, орієнтованих на всілякі екзотичні галузі, наприклад космічну фотозйомку. Частіше використовується його найпростіший і найнадійніший варіант, без стиснення і втрати даних. Хоча при цьому створюються великі файли, які часом нелегко вмістити на носіях.

Для скорочення витрат на графіку було розроблено спеціальні форми стиснення файлів.

JPG – базується на першому міжнародному стандарті для збереження зображень із деякою втратою якості *JPEG* (Joint Photographic Expert Group). Стиснення засноване на усередненні кольору сусідніх пікселів (інформація про яскравість при цьому не усереднюється) і відкиданні високочастотних складових в просторовому спектрі фрагмента зображення. Головним чином він призначений для фото, характерною рисою яких є плавні переходи напівтонів і розмиття чітких ліній.

GIF – формат обміну графікою (Graphic Interchange Format), навпаки, призначений для малюнків з чіткими кольорами та контурами, і економія досягається частково за рахунок мінімізації палітри.

PNG (Portable Network Graphic) – також орієнтований на малюнки з чіткими лініями, але не накладає обмежень на розміри палітри і базується на досконаліших загальнодоступних алгоритмах стиснення даних.

Для зменшення обсягу файлів за рахунок усунення повторів даних широко використовуються програми-архіватори, що забезпечують повне збереження «запакованої» інформації. Графічні файли у форматах *jpg* та *gif* практично не стискаються. Зате у десятки разів можуть бути «спресовані» стандартними архіваторами розлогі файли типів *bmp* або *tif*, що зумовлює їх велику розповсюдженість у користуванні.

1.4.3. Огляд моделей представлення кольору

Для завдання відповідності між кольорами, що сприймаються людиною та зберігаються в пам'яті, і кольорами, що формуються на пристроях виводу, використовується колірна модель.

Колірна модель – абстрактна модель опису представлення кольорів у вигляді кортежів (наборів) чисел, зазвичай з трьох або чотирьох значень, що називаютья колірними компонентами або колірними координатами. Разом з методом інтерпретації цих даних (наприклад, визначення умов відтворення та/або перегляду – тобто завдання способу реалізації), множина кольорів колірної моделі визначає колірний простір [32].

Колірний простір – модель представлення кольору, заснована на використанні колірних координат. Кольорова палітра будується таким чином, щоб будь-який колір був представлений точкою, що має певні координати. Найчастіше одному набору координат буде відповідати один колір, але для деяких випадків це не так.

RGB (Red, Green, Blue – червоний, зелений, синій) – адитивна колірна модель, що описує спосіб синтезу кольору, за якою червоне, зелене та синє світло накладаються разом, змішуючись у різноманітні кольори. Широко застосовується в техніці, що відтворює зображення за допомогою випромінення світла.

У даній моделі колір кодується градаціями складових каналів (Red, Green, Blue). Тому за збільшення величини градації котрогось каналу – зростає його інтенсивність під час синтезу.

Кількість градацій кожного каналу залежить від розрядності бітового значення *RGB*. Зазвичай використовують 24-бітну модель, у котрій визначається по 8 біт на кожен канал, і тому кількість градацій дорівнює 256, що дозволяє закодувати 256^3 = 16 777 216 кольорів (рис. 1.12).

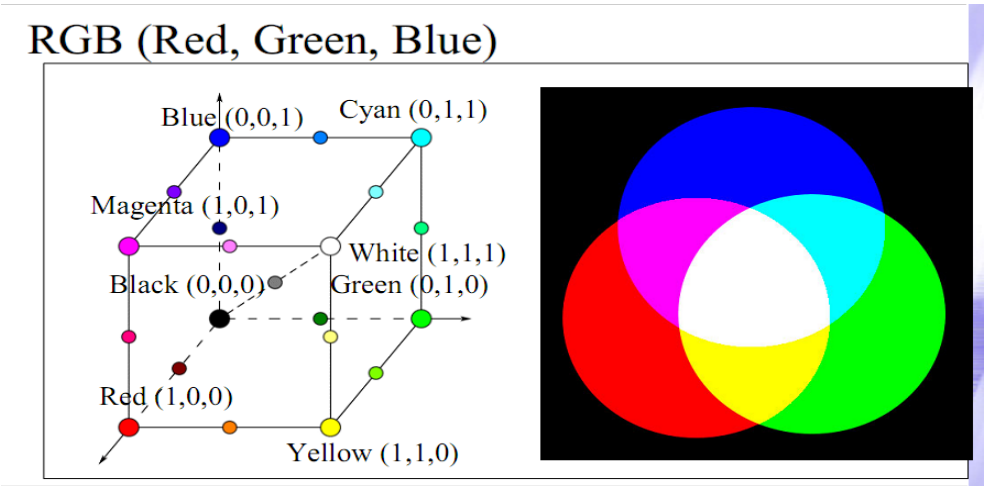


Рис. 1.12. Колірна модель *RGB*

Колірна модель *RGB* призначена сприймати, представляти та відображати зображення в електронних системах, таких як телебачення та комп'ютери, а також її застосовують у традиційній фотографії.

CMYK (Cyan, Magenta, Yellow, BlacK color – ціан, маджента та жовтий) – субтрактивна колірна модель, що використовується у поліграфії, перш за все при багатофарбовому (повноколірному) друці. Вона застосовується у друкарських машинах і кольорових принтерах.

Кожен колір в *CMYK* описується сукупністю чотирьох чисел, які називають колірними координатами. Кожне з цих чисел є відсотком фарби даного кольору у складовій колірної комбінації.

Модель *CMYK* враховує, яка кількість світла (і кольору) відбилася від тієї або іншої поверхні. Таким чином, якщо відняти з білого три первинні кольори, *RGB*, отримується трійка доповнюючих кольорів *CMY*. «Субтрактивний» означає той, що «віднімається».

Модель *CMYK* забезпечує менше колірне охоплення, ніж адитивна модель *RGB* (рис. 1.13).

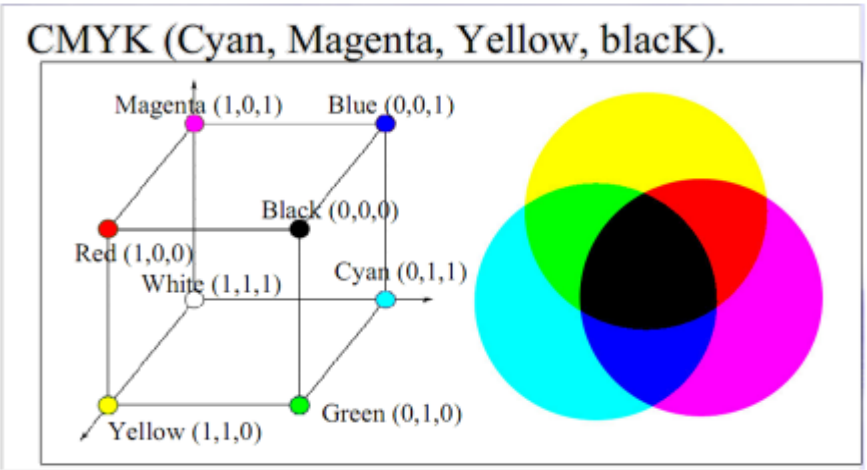


Рис. 1.13. Колірна модель *CMYK*

YCbCr – сімейство колірних просторів, які використовуються для передачі кольорових зображень у компонентному відео і цифровій фотографії. *Y* – компонента яскравості, а *Cb* і *Cr* є синьою і червоною кольорорізницевими компонентами (рис. 1.14).

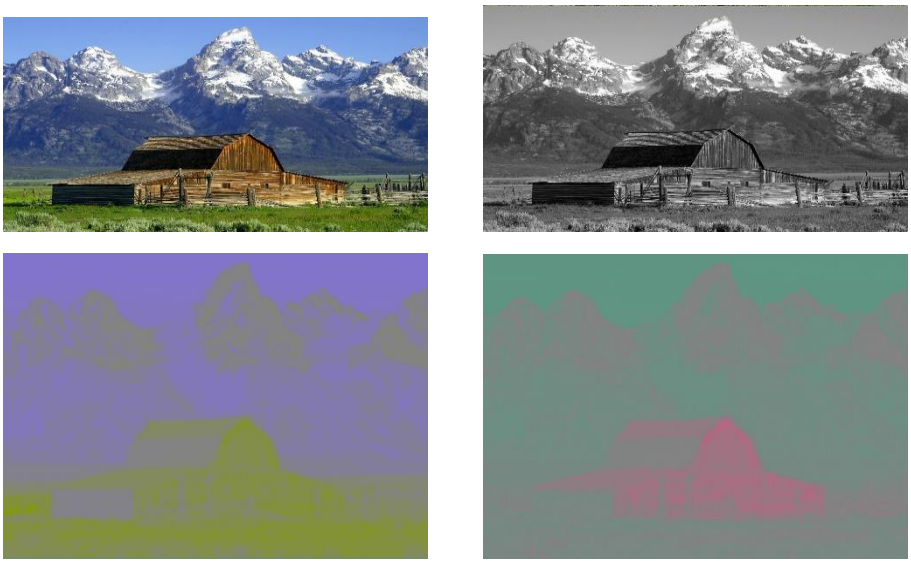


Рис. 1.14. Розкладання зображення на компоненти *Y*, *Cb* та *Cr*

YCbCr не є абсолютним колірним простором, скоріше, це спосіб кодування інформації сигналів *RGB*. Для систем відображення

використовуються сигнали основних кольорів *RGB* (червоний, зелений і синій). Ці сигнали не є ефективними для зберігання і передачі зображень, так як вони мають велику надмірність. Тому перехід у систему *YCbCr* дозволяє передати інформацію про яскравість з повною роздільною здатністю, а для кольоророзницевих компонент виконати субдискретизацію, тобто вибірку зі зменшенням числа переданих елементів зображення, так як людське око менш чутливе до перепадів кольору. Значення, виражене в *YCbCr* буде передбачуваним, якщо первинно використовувалися сигнали основних кольорів *RGB*. Перетворення компонент *RGB* у *YCbCr* відбувається наступним чином:

$$\begin{aligned} Y &= 16 + (65{,}481R + 128{,}553G + 24{,}966B), \\ Cb &= 128 + (-37{,}797R - 74{,}203G + 112B), \\ Cr &= 128 + (112R - 93{,}786G - 18{,}214B). \end{aligned} \tag{1.6}$$

1.4.4. Приклади зображень для дослідження

Зважаючи на розглянуті типи, формати і моделі цифрових зображень для досліджень були обрані растрові зображення формату *bmp* з глибиною кольору 24 біти та розміром 1024x1024 пікселів. Вибиралися кольорові зображення без різких переходів між текстурними областями та з достатньою кількістю мілких деталей (рис. 1.15).

Рис. 1.15. Приклади зображень для досліджень

1.5. Огляд існуючих стеганографічних методів

Найбільш поширені існуючі методи використовують просторову область і область перетворення для приховування інформації. Методи, які використовують область перетворення засновані на використанні дискретного косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), дискретного вейвлет-перетворення (ДВП), дискретного перетворення Карунена-Лоєва (ДКЛП) та інші. Такі перетворення можуть бути застосовані як до окремих частин зображення, так і для зображення в цілому.

Для досліджень був обраний найпоширеніший метод заміни найменш значущого біта (НЗБ) [25, 33], метод Куттера-Джордана-Боссена [25, 34], як один з кращих в просторової області, модифікований метод Коха-Жао [33, 35], як один з основних в частотній області, метод Бенгама, що є вдосконаленням попереднього [25, 36], метод, заснований на ДВП [37, 38, 39] та методи, засновані на розширенні спектра [40, 41, 42].

1.5.1. Методи приховування у просторову область

Методи, що використовують просторову область зображення вбудовують приховувані дані в області первинного зображення. Їх перевага полягає в тому,

що для вбудовування немає необхідності виконувати обчислювально складні і тривалі перетворення зображень.

Кольорове зображення *C* представлятимемо через дискретну функцію, яка визначає вектор кольору *c(x, y)* для кожного пікселя зображення *(x, y)*, де значення кольору задає трикомпонентний вектор в колірному просторі. Найпоширеніший спосіб передачі кольору – це модель *RGB*, в якій основні кольори – червоний, зелений і синій, а будь-який інший колір може бути представлений у вигляді зваженої суми основних кольорів.

Вектор кольору *c(x, y)* в *RGB*-просторі представляє інтенсивність основних кольорів. Повідомлення вбудовуються за рахунок маніпуляцій колірними складовими або безпосередньо яскравістю [25].

Загальний принцип цих методів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення. Для вилучення повідомлення необхідно знати алгоритм, за яким розміщувалася по контейнеру прихована інформація.

Метод заміни найменш значущого біта (*НЗБ*) найбільш розповсюджений серед методів заміни в просторовій області.

Молодший значущий біт зображення несе у собі найменше всього інформації. Відомо, що людина в більшості випадків не здатна помітити змінення в цьому біті. Фактично, НЗБ – це шум, тому його можна використовувати для вбудовування інформації шляхом заміни менш значущих бітів пікселів зображення бітами секретного повідомлення. При цьому, для зображення в градаціях сірого (кожний піксель зображення кодується одним байтом) об’єм вбудованих даних може складати 1/8 від загального об’єму контейнера. А якщо замінити два НЗБ, то пропускна здатність подвоюється (рис. 1.16).

Рис. 1.16. Приховування інформації методом НЗБ

Популярність даного методу зумовлена його простотою та тим, що він дозволяє приховувати у відносно невеликих файлах достатньо великі об’єми інформації (пропускна здатність прихованого каналу зв’язку, що створюється, складає при цьому 12,5 до 30%). Метод найчастіше працює з растровими зображеннями, представленими в форматі без компресії (наприклад *GIF* та *BMP*).

Метод вбудовує приховувані дані в області первинного зображення. Його перевага полягає в тому, що для вбудовування немає необхідності виконувати обчислювально складні і тривалі перетворення зображень (рис. 1.17) [2].

Рис. 1.17. Зміна кольору при заміні НЗБ

Основний недолік методу НЗБ – це низька стеганографічна стійкість до атак пасивного й активного порушників, тому що він має високу чутливість до найменших виправлень контейнера. Для ослаблення цієї чутливості часто додатково застосовують завадостійке кодування [33].

Метод Куттера-Джордана-Боссена (метод «хреста»). У даному методі запропоновано використовувати канал синього кольору зображення, що має *RGB*-кодування, для приховування інформації [25]. Оскільки ЗСЛ є найменш

чуттєвою до змін яскравості саме синього кольору у порівнянні з червоним та зеленим.

Вбудовування інформації відбувається у такий спосіб – один і-ий біт m_i повідомлення у один псевдовипадковий піксель контейнера $p = (x, y)$. Секретний ключ *K0* задає координати пікселів, у які буде приховуватися інформація. При вбудовування яскравості червоного та зеленого кольорів залишаються незмінними, а яскравість синього – змінюється за такою формулою:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \upsilon \cdot \lambda_{x,y}, при\ m_i = 0; \\ B_{x,y} - \upsilon \cdot \lambda_{x,y}, при\ m_i = 1. \end{cases}, \quad (1.7)$$

де $\lambda_{x,y} = 0.3 \cdot R_{x,y} + 0.59 \cdot G_{x,y} + 0.11 \cdot B_{x,y}$ – яскравість пікселя;

υ – коефіцієнт, що задає енергію біта даних, що вбудовуються (задається виходячи з функціонального призначення і особливостей стеганосистеми). Чим більше υ, тим вища стійкість вкладення, але тим більша помітність.

Оскільки на приймаючій стороні немає зображення-оригіналу, то гарантовано дізнатися у яку сторону змінилася яскравість синього кольору ми не можемо. Тому для вилучення прогнозується значення яскравості вихідного синього кольору на основі його сусідів:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma} (B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma}, \quad (1.8)$$

де $\sigma = 1 \div 3$ – розмір області, по якій буде прогнозуватися яскравість.

Піксель у центрі – це піксель, яскравість синього кольору якого ми повинні спрогнозувати спираючись на пікселі, які позначені світло-сірим кольором (рис. 1.18).

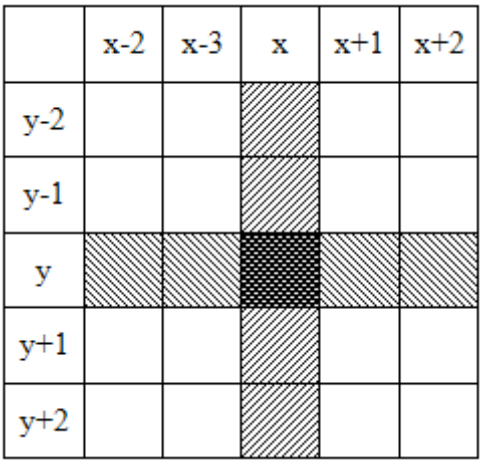


Рис. 1.18. Метод «хреста» при $\sigma = 2$

І нарешті, при вилученні прихованого біта обчислюється різниця δ між поточним ($B^*_{x,y}$) і зпрогнозованим ($\overline{B^*_{x,y}}$) значеннями інтенсивності пікселя $p = (x, y)$:

$$\delta = B^*_{x,y} - \overline{B^*_{x,y}}, \tag{1.9}$$

якщо $\delta < 0$, то $m_i = 0$;

якщо $\delta > 0$, то $m_i = 1$.

Перевагою цього методу є висока пропускна здатність, стійкість до несанкціонованого ознайомлення, до частотного детектування, до руйнування молодшого біта контейнера та до атак стискання.

Недоліком є те, що вилучення повідомлення має ймовірнісний характер [34]. Для зменшення ймовірності помилки використовується завадостійке кодування. Також можна у процесі вбудовування кожен біт повторювати декілька разів (багаторазове вбудовування).

1.5.2. Методи приховування в області перетворень

Стійкішими до різних спотворень, у тому числі і компресії, є методи, що використовують для приховання даних не просторову область контейнера, а частотну [33].

Існує декілька способів представлення зображення в частотній області. При цьому використовується та або інша декомпозиція зображення, що використовується як контейнер. Наприклад, існують методи засновані на використанні дискретного косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення Карунена-Лоєва і деяких інших. Подібні перетворення можуть застосовуватися або до окремих частин зображення, або до зображення в цілому.

Найбільшого поширення серед усіх ортогональних перетворень у стеганографії отримали вейвлет-перетворення і ДКП, що певною мірою пояснюється значним поширенням їх використання при компресії зображень [43]. Крім того, для приховання даних доцільно застосовувати саме те перетворення зображення, якому останнє піддаватиметься з часом при можливій компресії.

Ефективність вживання вейвлет-перетворення і ДКП для компресії зображень пояснюється тим, що вони добре моделюють процес обробки зображення в ЗСЛ, відокремленні значимих деталей від другорядних. Таким чином, зазначені перетворення доцільніше використовувати в разі присутності активного порушника, оскільки модифікація значимих коефіцієнтів може привести до неприйнятного викривлення зображення [44].

Під час цифрової обробки зображення часто застосовується двомірна версія дискретного косинусного перетворення:

$$\Omega(\upsilon,\nu)=\frac{\xi(\upsilon)\cdot\xi(\nu)}{\sqrt{2N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right];\quad(1.10)$$

$$S(x,y)=\frac{1}{\sqrt{2N}}\cdot\sum_{\upsilon=0}^{N-1}\sum_{\nu=0}^{N-1}\xi(\upsilon)\cdot\xi(\nu)\cdot\Omega(\upsilon,\nu)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right],\quad(1.11)$$

де *C(x, y)* і *S(x, y)* – відповідно, елементи оригінального і відтвореного за коефіцієнтами ДКП зображення розмірністю *NxN*;

x, y – просторові координати пікселів зображення;

Ω(υ, ν) – масив коефіцієнтів ДКП;

(υ, ν) – координати в частотної області;

$\xi(\upsilon)=\frac{1}{\sqrt{2}}$, якщо $\upsilon\approx 0$, і $\xi(\upsilon)=1$, якщо $\upsilon>0$.

Метод відносної заміни величин коефіцієнтів ДКП (метод Коха і Жао). Один з найпоширеніших на сьогодні методів приховання конфіденційної інформації в частотної області зображення полягає у відносній заміні величин коефіцієнтів ДКП [25, 35].

На початковому етапі первинне зображення розбивається на блоки розмірністю *8x8* пікселів. ДКП застосовується до кожного блоку (1.10), внаслідок чого отримують матриці *8x8* коефіцієнтів ДКП, які часто позначають $\Omega_b(\upsilon, \nu)$, де *b* – номер блоку контейнера *C*, а *(υ, ν)* – позиція коефіцієнта в цьому блоці. Кожен блок при цьому призначений для приховання одного біта даних.

Під час організації секретного каналу абоненти повинні завчасно домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які використовуватимуться для приховання даних. Коефіцієнти задаються координатами в масивах коефіцієнтів ДКП: (υ_1, ν_1) і (υ_2, ν_2). Окрім цього, вказані коефіцієнти повинні відповідати косинус-функціям з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЛ областях сигналу, до того ж інформація не спотворюватиметься при *JPEG*-компресії з малими коефіцієнтами стиснення [33].

Безпосередньо процес приховання починається з випадкового вибору блоку C_b зображення, призначеного для кодування b-го біта повідомлення. Вбудовування інформації здійснюється таким чином: для передачі біта «0» прагнуть, щоб різниця абсолютних значень обраних коефіцієтів ДКП перевищувала деяку позитивну величину, а для передачі біта «1» ця різниця робиться меншою в порівнянні з деякою негативною величиною P:

$$\begin{cases} \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| > P, при\ m_b = 0; \\ \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| < -P, при\ m_b = 1 \end{cases} \quad (1.12)$$

Таким чином, первинне зображення спотворюється за рахунок внесення змін до коефіцієнтів ДКП, якщо їх відносна величина не відповідає приховуваному біту. Чим більше значення P, тим стеганосистема, створені на основі даного методу, є стійкішою до компресії, проте якість зображення при цьому значно погіршується. Після відповідного внесення корекції в значення коефіцієнтів, які повинні задовольняти нерівності, проводиться зворотнє ДКП за формулою (1.11).

Для вилучення даних, в декодері виконується аналогічна процедура вибору коефіцієнтів, а рішення про переданий біт приймається у відповідності з наступним правилом:

$$\begin{cases} m_b^* = 0, при\ \left|\Omega_b^*(\upsilon_1,\nu_1)\right| > \left|\Omega_b^*(\upsilon_2,\nu_2\right| \\ m_b^* = 1, при\ \left|\Omega_b^*(\upsilon_1,\nu_1)\right| < \left|\Omega_b^*(\upsilon_2,\nu_2\right| \end{cases} \quad (1.13)$$

Метод Бенгама – Мемона – Ео – Юнга є оптимізованою версією вищерозгляненого методу [36]. Причому оптимізація була проведена по двох напрямках: по-перше, було запропоновано для вбудовування використовувати не всі блоки, а лише найбільш підходящі для цього, по-друге, в частотної

області блоку для вбудовування вибираються не два, а три коефіцієнти ДКП, що істотно зменшує візуальні спотворення контейнера [33].

Придатними для вбудовування інформації вважаються такі блоки зображення, які одночасно задовольняють наступним двом умовам:

– блоки не повинні мати різких переходів яскравості,

– блоки не мають бути дуже монотонними.

Блоки, які не відповідають першій вимозі, характеризуються наявністю дуже великих значень низькочастотних коефіцієнтів ДКП, зрівнянних за величиною з ДК-коефіцієнтом. Для блоків, які не задовольняють другій вимозі, характерна рівність нулю більшості високочастотних коефіцієнтів. Вказані особливості виявляються критерієм відбракування непридатних блоків.

Відмічені вимоги відбракування враховуються використанням двох порогових коефіцієнтів: P_L (для першої вимоги) і P_H (для другої вимоги), перевищення (P_L) або недосягнення (P_H) яких вказуватиме на те, що даний блок не придатний для модифікації в частотної області.

Вбудовування в блок біта повідомлення здійснюється таким чином. Вибираються (для більшої стійкості стеганосистеми – псевдовипадково) три коефіцієнти ДКП блоку з середньочастотної області з координатами, (υ_1, ν_1) і (υ_2, ν_2). Якщо необхідно провести вбудовування «0», ці коефіцієнти змінюються так, щоб третій коефіцієнт став менше будь-якого з перших двох, якщо необхідно приховати «1», він робиться великим у порівнянні з першим і другим коефіцієнтами:

$$\begin{cases} \left|\Omega_b(\upsilon_3,\nu_3)\right| < \left|\Omega_b(\upsilon_1,\nu_1\right|; \\ \left|\Omega_b(\upsilon_3,\nu_3)\right| < \left|\Omega_b(\upsilon_2,\nu_2\right|. \end{cases}, \textit{ при } m_b = 0; \\ \begin{cases} \left|\Omega_b(\upsilon_3,\nu_3)\right| > \left|\Omega_b(\upsilon_1,\nu_1\right|; \\ \left|\Omega_b(\upsilon_3,\nu_3)\right| > \left|\Omega_b(\upsilon_2,\nu_2\right|. \end{cases}, \textit{ при } m_b = 1. \tag{1.14}$$

Як і в попередньому методі, для ухвалення рішення про достатність розрізнення вказаних коефіцієнтів ДКП, у вираз (1.13) вводиться значення порогу розрізнення *P*:

$$\begin{cases} \left|\Omega_b(\upsilon_3,\nu_3)\right| < \mathbf{min}(\left|\Omega_b(\upsilon_1,\nu_1\right|,\left|\Omega_b(\upsilon_2,\nu_2\right|) - P, \textit{при } m_b = 0; \\ \left|\Omega_b(\upsilon_3,\nu_3)\right| > \mathbf{max}(\left|\Omega_b(\upsilon_1,\nu_1\right|,\left|\Omega_b(\upsilon_2,\nu_2\right|) - P, \textit{при } m_b = 1. \end{cases} \quad (1.15)$$

У тому випадку, якщо така модифікація призводить до дуже великої деградації зображення, коефіцієнти не змінюють, і блок як контейнер не використовується.

Використання трьох коефіцієнтів замість двох і, що найголовніше, відмова від модифікації блоків зображення в разі неприйнятних їх викривлень, зменшує погрішності, які вносяться повідомленням. Одержувач завжди може визначити блоки, в які не проводилося вбудовування, просто повторивши аналіз, аналогічний виконаному на передавальній стороні.

Методи на основі дискретного вейвлет-перетворення (ДВП).

Вейвлет-перетворення – це локалізований аналітичний метод часових інтервалів із фіксованим розміром вікна й конвертованою формою, що дає змогу добре локалізувати низькочастотні деталі сигналу в частотній області (основні гармоніки), а високочастотні – в часовій [37, 39]. Основна ідея дискретного вейвлет-перетворення у процесі обробки зображення полягає в розкладанні зображення на часткові зображення різних просторових та частотних областей.

Після ДВП інформація аналізується в 4-х частотних областях, одна з яких є низькочастотною (LL) і три – високочастотними (LH, HL, HH) (рис. 1.19).

Як правило, для приховування водяних знаків використовується високочастотні складові, оскільки людське око менш чутливе до змін у цих областях [39]. Але область LL є відносно стійкішою, бо вона містить переважну

більшість енергії зображення. Для того, щоб отримати кращий показник стійкості, водяний знак вбудовується саме у це часткове зображення.

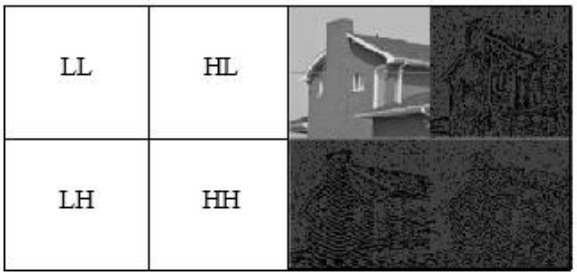


Рис. 1.19. Перший рівень вейвлет-перетворення

При 2-рівневому розкладанні спочатку виконується ДВП у вертикальному напрямку, а потім ДВП у горизонтальному напрямку для кожного з рівнів. Після першого рівня розкладання утворюється 4 піддіапазони: LL_1, LH_1, HL_1 та HH_1. Для кожного наступного рівня розкладання в якості вихідного зображення використовується LL піддіапазон. Отже, для виконання другого рівня розкладання ДВП застосовується до LL_1 діапазону, що призводить до його перетворення на чотири піддіапазони: LL_2, LH_2, HL_2, і HH_2.

Для здійснення 3-рівневого розкладання ДВП застосовується до LL_2 діапазону, що розкладає його на чотири піддіапазони – LL_3, LH_3, HL_3, HH_3. Це призводить до утворення 10-ти піддіапазонів одного компоненту. LH_1, HL_1, і HH_1 містять найбільш високі частотні складові зображення, а LL_3 – найнижчі. 3-рівневе ДВП розкладання показано на рис. 1.20.

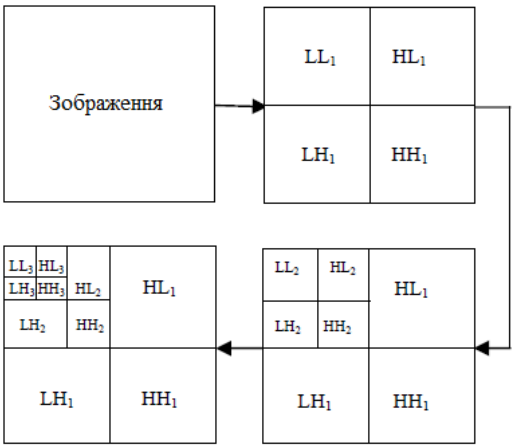


Рис. 1.20. 3-рівневе дискретне вейвлет розкладання

Для дискретного вейвлет-аналізу використовують різні базиси вейвлетів, зокрема вейвлети Хаара, Добеші, симлети, кофлети та ортогональні вейвлети. Наведені базиси відрізняються різними значеннями вейвлет-коефіцієнтів та підходами до формування спектрів.

В реалізації методу, що наведений в Додатку Б, використовуються вейвлети Добеши. Як метод вбудовування ЦВЗ використовується альфа-змішування. Тобто компоненти вейвлет розкладання вихідного зображення та ЦВЗ множаться на коефіцієнт масштабування та додаються. У формулі (1.16) подається зображення із ЦВЗ, як результат альфа-змішування.

$$WMI = k \cdot (LL3) + q \cdot (WM3), \tag{1.16}$$

де *WMI* – низькочастотна складова заповненого зображення,

LL3 – низькочастотна складова вихідного зображення, отриманого за допомогою 3-рівневого ДВП,

WM3 – низькочастотна складова ЦВЗ,

k, *q* – коефіцієнти масштабування для вихідного зображення і ЦВЗ відповідно.

Після вбудовування ЦВЗ у зображення-контейнер виконується зворотне 3-рівневе ДВП коефіцієнтів отриманого зображення з метою отримання кінцевого захищеного ЦВЗ зображення.

Методи розширення спектру. Для досліджень було обрано два методи, які вбудовують водяний знак шляхом модуляції коефіцієнтів ДКП (рис. 1.21) [40]. Бо вони мають найбільш високі показники стійкості серед методів розширення спектру. Перший метод був описаний доктором Руні [41] і заснований на модуляції середньої смуги частот окремих блоків зображення за допомогою випадкового Гауссівського сигналу. Другий метод згідно Піва та ін. [42] також модулює коефіцієнти ДКП, але використовує інший частотний діапазон більш низьких частот. Стійкість водяного знаку надалі корегується згідно з перцепційною маскою.

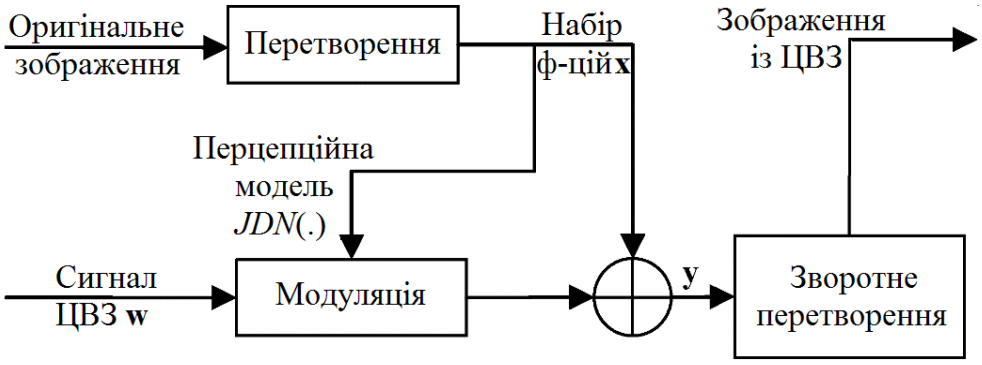


Рис. 1.21. Принцип методів з розширенням спектру

Метод 1: зображення спочатку ділиться на блоки *128×128*. Над кожним блоком здійснюється ДКП , коефіцієнти отримуються зигзагоподібно, як при *JPEG* стисненні. Середні 30% коефіцієнтів D_k модулюються гаусівським сигналом S_k з нульовим середнім, шляхом простого додавання обох сигналів:

$$D'_k = D_k + \alpha S_k, \quad k = 1, \ldots, N_m, \tag{1.17}$$

де D'_k – змінені ДКП коефіцієнти,

α – енергія ЦВЗ,

N_m – число змінених коефіцієнтів.

Маркований ЦВЗ блок отримується шляхом виконання зворотного ДКП з використанням змінених коефіцієнтів D'_k. Конкретний частотний діапазон обирається як компроміс між невидімістю та стійкістю ЦВЗ.

Одну з версій методу було пояснено у [41]. В [41] передбачалося, що інформація, що складає ЦВЗ складається з M символів і кожен символ s_i представляється за допомогою r біт, $1 \le s_i \le 2^r$. Для кожного i генерується послідовність $\xi^{(i)}$ з псевдовипадкових величин довжиною N_m+2^r рівномірно розподілених у [−1, 1]. Кожен символ s представляється сегментом $\eta^{(i)} = \xi_s^{(i)}, \ldots, \xi_{s+N_m-1}^{(i)}$ послідовних N_m псевдовипадкових чисел. Для кожного символу генерується нова псевдовипадкова послідовність (ПВП). Результат генерації псевдовипадкового шуму використовується в якості ключа. Тоді повідомлення з M символів можна представити сумою:

$$S = \sqrt{\frac{3}{M}} \sum_{i=1}^{M} \eta^{(i)}. \qquad (1.18)$$

Сигнал з розширеним спектром S є приблизно Гауссовим з нульовим середнім і одиничним стандартним відхиленням дисперсією стандартного відхилення навіть при помірних значеннях M (наприклад, $M \approx 10$).

Метод 2 був представлений і досліджений у ряді публікацій Піва та ін. [40, 42]. І нещодавно був розширений ДПФ. Зображення перетворюється з використанням ДКП, де коефіцієнти отримуються зигзагоподібно. Перші M коефіцієнтів пропускаються (щоб уникнути створення видимих артефактів), а наступні L коефіцієнтів змінюються, використовуючи наступне правило:

$$D'_k = D_k + \alpha \mid D_k \mid S_k, \quad k = 1, \ldots, N_m, \qquad (1.19)$$

де α – енергія ЦВЗ,

S_k – гаусовська послідовність $N(0,1)$.

Числа M і L залежать від розмірів зображення і можуть бути підлаштовані для досягнення компромісу між стійкістю і видимістю ЦВЗ. Знову ж таки, модифіковане зображення I_m отримується шляхом обчислення зворотного ДКП з використанням замінених ДКП коефіцієнтів D'_k. Наступним кроком зображення із ЦВЗ I_w обчислюється як випукла комбінація зміненого зоюраження I_m і вихідного зображення I (додавання відбувається піксель за пікселем):

$$I_w = s\, I_m + (1-s)\, I. \tag{1.20}$$

Вага s пікселя (i, j) обчислюється як локальне стандартне відхилення $\sigma(i, j)$ пікселя (i, j), розраховане в квадраті 9×9 з центром у (i, j), розділене на максимальне стандартне відхилення у всьому зображенні $max_{i,j}\ \sigma(i, j)$. Ця випукла комбінація підлаштовує енергію ЦВЗ до локальних властивостей зображення.

1.6. Висновки до першого розділу

У першому розділі дисертаційної роботи були отримані наступні результати:

1. Визначені основні сфери використання, характеристики та методи стеганографії. Обґрунтована актуальність її використання для вирішення сучасних задач, пов’язаних з прихованою передачею інформації та захистом авторських прав.

2. Адаптована математична модель стеганосистеми як системи передачі інформації, що описує передачу повідомлення від відправника до отримувача, до вимог дисертаційної роботи, шляхом врахування навмисних атак та випадкових завад.

3. Наведено класифікацію показників, що дають кількісні та якісні оцінки для порівняльного оцінювання якості стеганографічних засобів. До кількісних оцінок, що оперують із зображеннями на рівні пікселів, відносяться співвідношення «сигнал/шум», нормована середня абсолютна різниця, якість зображення, середньоквадратична похибка та середня абсолютна різниця. До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, відносяться: пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення.

4. Виконано обґрунтування вибору типу зображень для досліджень. Були обрані кольорові *bmp* зображення з глибиною кольору 24 біти та розміром *1024x1024* пікселів. Акцент робиться на групі кольорових зображень без різких переходів між текстурними областями, що мають достатню кількість мілких деталей.

5. Для досліджень були обрані та коротко охарактеризовані наступні методи: найпоширеніший метод заміни найменш значущого біту, метод Куттера-Джордана-Боссена, як один з кращих в просторової області, модифікований метод Коха-Жао, як один з основних в частотній області, метод Бенгама, що є вдосконаленням попереднього, метод, заснований на ДВП та методи із розширенням спектра сигналу.

РОЗДІЛ 2
ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ

2.1. Математичний апарат для багатокритеріальної оптимізації

Для визначення оптимального стеганографічного методу для прихованої передачі даних по мережах зв'язку необхідно здійснити експертне оцінювання існуючих методів за обраними критеріями.

Експертне оцінювання стеганографічних методів проводиться відповідною експертною групою, до складу якої входять незалежні фахівці. В ході експертизи різноманітні параметри підлягають оцінці з боку експертної групи і в подальшому виникає необхідність обробки отриманих даних з метою їх узагальнення та формування кінцевих результатів експертизи. Початковою інформацією для обробки є судження, що відображають переваги метода у числовій і лінгвістичній формі, тому є необхідність використання якісних і кількісних методів обробки результатів експертної оцінки. Кількісні методи є більш зручними з точки зору їх застосування під час такого оцінювання [45]. Для агрегації результатів експертизи виникає необхідність використання параметру, який би відображав оцінку експерта. Ним може бути коефіцієнт важливості (КВ), який широко використовується для побудови рішення в багатокритеріальних задачах [46, 47, 48] та математичному програмуванні [49, 50].

Отже, необхідно здійснити дослідження сучасних методів розрахунку КВ та визначити найбільш доцільний для подальшого використання у дослідженнях методів вбудовування інформації. Метод багатокритеріальної оцінки буде використовуватися для визначення КВ критеріїв, за якими оцінюються стеганографічні методи, а згодом для комплексного порівняльного аналізу методів приховування в конкретних умовах проведення експертизи.

2.1.1. Стислий огляд найпоширеніших методів визначення коефіцієнтів важливості

Всі методи визначення пріоритету критеріїв (важливості критеріїв, обробки результатів експертизи, формування експертних суджень) прийнято поділяти на якісні та кількісні відповідно до інформації, яка надходить від експертів (вербальна або кількісна). Якісні методи придатні для тих випадків, коли метою експертизи є отримання якісних оцінок певних критеріїв об'єкту, визначення найкращої альтернативи, а кількісна характеристика носить другорядний характер. В іншому випадку, коли необхідно отримати числові оцінки, використовують кількісні методи.

До *якісних методів* визначення пріоритету критеріїв відносять методи «Делфі» [51], ранжування [51], бінарних [52] та множинних порівнянь [51], нормалізації [53], вектору переваг [52], а також кластерного аналізу [54].

Кількісні методи визначення пріоритету критеріїв прийнято розділяти на п'ять груп: попарних порівнянь [55, 56, 57, 58, 59, 60], рангових перетворень [52], [55, 61, 62, 63, 64], апроксимації функції корисності [46, 52, 66, 67, 68], трансформації частот [46, 50, 68, 69] та відхилення від точки рівноваги [58, 70, 71, 72].

Найбільш повний огляд методів визначення коефіцієнтів важливості наведений у літературі [51].

Для розрахунку вагових коефіцієнтів використовуються різні підходи, у рамках яких розроблено безліч різноманітних методів [73]. Проаналізуємо лише основні підходи.

Пряма розстановка. Експерти розставляють ваги факторам, виходячи з деякої вимоги, наприклад, щоб сума усіх ваг була рівна одиниці або 100%, хоча може бути обрана і будь-яка інша константа, якщо це виявиться зручніше для подальших розрахунків.

Труднощі цього підходу полягають у необхідності у неявному вигляді тримати у полі зору одночасно усі фактори, оскільки, присвоюючи певне

числове значення конкретному фактору, експерт повинен одночасно його співставити з усіма іншими. Труднощі зростають у геометричній прогресіїї зі збільшенням числа факторів.

Є ще й технічне ускладненя у роботі експерта, пов'язане з необхідністю постійно контролювати поточну суму вагових коефіцієнтів, щоб не опинитися перед фактом перевищення заданої константи або залишити на останні фактори занадто велику частину. Якщо це відбувається, то доводиться перевизначати вже присвоєні коефіцієнти, що може відбуватися декілька разів, поки цей своєрідний ітераційний процес не скінчиться. Число ітерацій збільшується зі зростанням кількості факторів.

Ранжування факторів. Цей підхід дещо полегшує експертам роботу, оскільки не потребує контролю загальної суми коефіцієнтів. Тут від експертів вимагається провести ранжування, тобто впорядкувати фактори, що досліджуються, за ступенем проявлення їх властивостей у порядку їх зростання або спадання.

$$\begin{cases} R_{11}, R_{21}, \dots, R_{n1}; \\ R_{12}, R_{22}, \dots, R_{n2}; \\ \dots\dots\dots\dots\dots\dots; \\ R_{1m}, R_{2m}, \dots, R_{nm}; \end{cases} \qquad (2.1)$$

де R_{ij} – ранг (місце), присвоєне фактору O_i j-м експертом у ряді з n досліджених об'єктів, впорядкованих цим експертом за ступенем прояву властивості, що аналізується. Допускається двом чи більше факторам присвоювати однаковий ранг, але тоді він буде дробовим. Зведену оцінку вагових коефіцієнтів можна отримати у результаті усереднення окремих рангів по стовпцям.

Перевага цього методу полягає у його простоті, але це не той випадок, коли простота ефективна, оскільки усереднення рангів призводить до більш грубих оцінок вагових коефіцієнтів порівнянно з іншими методами. Окрім того, він також не звільняє експерта від необхідності тримати у полі зору усі

фактори, як і при прямій розстановці.

Присвоєння коефіцієнтів факторам. У цьому методі експертам пропонується оцінити фактори по деякій бальній шкалі, наприклад від 1 до 10. Тоді отримуємо вираз:

$$\begin{cases} y_{11}, y_{21}, \dots, y_{n1}; \\ y_{12}, y_{22}, \dots, y_{n2}; \\ \dots\dots\dots\dots\dots; \\ y_{1m}, y_{2m}, \dots, y_{nm}; \end{cases} \tag{2.2}$$

де y_{ij} – бальна оцінка фактору, отримана від j-го експерта,

n – кількість факторів,

m – число експертів.

Зведені оцінки вагових коефіцієнтів зазвичай знаходять шляхом підбору відповідної регресійної моделі. Середню оцінку w_i вагових коефіцієнтів факторів можливо отримати за простими формулами:

$$w_i = \frac{\sum_{j=1}^{m} w_{ij}}{\sum_{j=1}^{m}\sum_{i=1}^{n} w_{ij}}, \tag{2.3}$$

де w_{ij} – вага i-го об’єкту, розрахована за оцінками усіх експертів;

$$w_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}}, \tag{2.4}$$

де x_{ij} – оцінка фактору i, що дана експертом j;

n – число факторів,

m – число експертів.

Цей метод у деякій мірі робить слабшою залежність оцінки конкретного фактору від інших, але остаточно не звільняє від неї, оскільки фактори все ж потрібно співставляти – інакше коефіцієнти важливості неможливо коректно розставити.

Метод аналізу ієрархій. Частково уникнути вказаних вище складностей покликаний метод аналізу ієрархій (MAI), розроблений Т. Сааті [74] у 80-х роках минулого століття. Суть методу полягає у попарному порівнянні факторів відносно один одного за впливом на кінцеву ціль. При цьому вплив інших факторів не враховується. Для попарного порівняння факторів Сааті запропонував спеціальну оціночну шкалу, що складається з п’яти основних та чотирьох проміжних суджень. Згідно з нею судження експерів представляються у наступному вигляді (табл. 2.1).

Таблиця 2.1

Ієрархія експертних порівнянь співвідношення факторів

Судження	Пояснення
1. Рівна важливість	Рівний вклад факторів у ціль
3. Помірна перевага	Досвід і судження дають легку перевагу одного фактору над іншим
5. Суттєва перевага	Досвід і судження дають сильну перевагу одного фактору над іншим
7. Значна перевага	Одному фактору дається настільки сильна перевага, що вона стає практично значимаю
9. Дуже сильна перевага	Очевидність переваги одного фактору над іншим підтверджується найбільш сильно
2, 4, 6, 8. Проміжне судження	Застосовується у компромісному випадку

У підсумку результати парних порівнянь представляються у вигляді квадратної матриці $A=(a_{ij})$ з одиничною діагоналлю (порівняння фактору самого з собою дорівнює одиниці). Тут (a_{ij}) означає відношення оцінок відповідних елементів; індекси *i* и *j* змінюються від одиниці до велечини, що дорівнює кількості факторів. Оскільки при послідовному переборі усіх можливих пар фактори порівнюються між собою двічі (спочатку – фактор a_i з фактором a_j, потім – у зворотному порядку), при складанні матриці повинно виконуватися умова «оберненої симетричності»: $a_{ji}=\frac{1}{a_{ij}}$. Із цього випливає, що достатньо заповнювати лише одну частину матриці – ту, що лежить вище або нижче діагоналі, це не має принципового значення внаслідок елементарного перерахунку взаємно обернених значень. Якщо розглядати *n* факторів, то всього можлива наявність $\frac{n^2-n}{2}$ значень комбінацій.

В MAI для кодування використовується номер судження рядка табл. 2.1. Кожне з приведених суджень кодується числом від 1/9 до 9. Наприклад, якщо надано значну перевагу елемента A_i (наприклад, стійкість стеганографічної системи для прихованої передачі даних) над елементом A_j (наприклад, пропускна здатність стеганографічної системи для прихованої передачі даних), то вважають, що в матриці парних порівнянь a_{ij} = 5 і відповідно a_{ji} = 1/5, оскільки для кодування використовується п’яте судження.

Суть обробки матриці полягає у розкладанні:

$$A \approx Z \cdot U, \tag{2.5}$$

де $U=\left(\frac{1}{z_1},...,\frac{1}{z_n}\right)$.

Мета – визначення компонент вектора ваг $Z=(z_1,...,z_n)$, що дозволяє ранжувати фактори A_i.

Розрахунок ваг можна здійснити кількома способами. Одним з можливих підходів до апроксимації вектора ваг може слугувати розрахунок власного вектора матриці парних порівнянь, який дорівнює відповідному максимальному власному числу. Відповідні алгоритми знаходження власного вектору достатньо детально розроблені, і їх опис можна знайти зокрема в монографіях [75, 76].

Процедура MAI має в своєму розпорядженні вбудований критерій якості роботи експерта – індекс узгодженості (ІУ), який дає інформацію про ступінь порушення чисельної (кардинальної) і транзитивної (порядкової) узгодженості експертних суджень. [77]. Перевірка на кардинальність полягає у контролі певних числових характеристик, відхилення від яких свідчитиме про наявність помилок при формалізації експертних суджень. Іншими словами, якщо прийняті деякі правила кодування експертних суджень, наприклад, від нуля до одиниці, то експертні судження не повинні виходити за рамки встановленої цим правилом множини значень, тобто бути від'ємними чи більше одиниці. Транзитивність дозволяє перевірити логіку мислення експерта. Якщо експерт вважає, що фактор А переважає фактор Б, а фактор Б, в свою чергу, переважає фактор В, то при парному порівнянні фактор В не повинен переважати фактор А, тобто повинна виконуватися нерівність А > Б > В.

Відсутність узгодженості може бути серйозним обмежуючим фактором для дослідження деяких проблем. ІУ у кожній матриці можна оцінити за формулою:

$$ІУ = \frac{\lambda - n}{n - 1}, \tag{2.6}$$

де λ – власне число,

n – число факторів, що порівнюються.

Якщо порівняти ІУ з деякою величиною, отриманою при випадковому виборі кількісних оцінок, то можна знайти критерій якості роботи експерта.

Розробник методу рекомендував визначені значення для оцінки середньої узгодженості (СУ) випадкових матриць різного порядку [74]. Але згодом, Донеганом та Доддом [78] були проведені додаткові дослідження, що підвищили точність отриманих оцінок, наведених у табл. 2.2.

Таблиця 2.2

Середні узгодженості (СУ) для випадкових матриць різного порядку

n	1	2	3	4	5	6	7	8	9	10
СС	0	0	0,49	0,80	1,06	1,18	1,25	1,32	1,37	1,41

Якщо розділити ІУ на СУ для матриці того ж порядку, то отримаємо відношення узгодженності (ВУ):

$$ВУ = \frac{ІУ}{СУ} \cdot 100\%. \qquad (2.7)$$

Якість експерта оцінюється за величиною ВУ. За рекомендацією Сааті величина відношення узгодженності повинна бути порядка 10% або менше, щоб бути задовільною. У деяких випадках можливо допустити 20%, але не більше. Якщо відношення узгодженності виходить за ці межі, то результати роботи таких експертів повинні бути виключені з розгляду.

2.1.2. Розрахунок оцінок вагових коефіцієнтів різними методами багатокрітеріальної оптимізації

Незалежно від кількості впливаючих факторів судження експертів будуть розходитися. Тому необхідне узагальнення оцінок індивідуальних експертів, результуюча величина яких і використовується безпосередньо в наукових і прикладних дослідженнях [79].

Залежність значень вагових коефіцієнтів від способу розрахунку та

обробки експертних суджень покажемо на даних, отриманих у процесі аналізу вимог до стеганографічних методів приховування даних при передачі мережами зв’язку. З робіт визнаних експертів зі стеганографії [24, 80, 81, 82, 83] були визначені взаємні значення факторів методом аналізу ієрархій, прямої розстановки ваг у вигляді процентів і ранжування факторів за їх значимістю.

Оброблені результати експертних оцінок наведені у табл. 2.3, де у стовпцях вказані значення вагових коефіцієнтів, розрахованих шляхом використання трьох методів: MAI, ранжування (Р) і прямої розстановки (ПР).

Таблиця 2.3

Вагові коефіцієнти, розраховані трьома методами

	Фактори	Експерти														
		1			2			3			4			5		
		MAI	Р	ПР	MAI	Р	ПР	MAI	Р	ПР	MAI	Р	ПР	MAI	Р	ПР
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	Пропускна здатність	0,32	0,24	0,30	0,29	0,24	0,20	0,41	0,29	0,40	0,18	0,19	0,20	0,31	0,26	0,31
2	Стійкість	0,02	0,05	0,02	0,03	0,05	0,02	0,02	0,05	0,02	0,01	0,05	0,04	0,03	0,05	0,03
3	Невидимість	0,30	0,24	0,25	0,30	0,24	0,40	0,29	0,21	0,30	0,33	0,24	0,25	0,29	0,19	0,28
4	Захищеність	0,29	0,24	0,28	0,30	0,24	0,30	0,21	0,21	0,20	0,41	0,29	0,40	0,30	0,26	0,30
5	Складність вбудовування	0,04	0,10	0,10	0,04	0,12	0,04	0,04	0,14	0,04	0,04	0,12	0,01	0,04	0,14	0,05
6	Складність вилучення	0,04	0,14	0,05	0,04	0,12	0,04	0,03	0,10	0,04	0,04	0,12	0,10	0,04	0,10	0,04

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

$$r = \frac{n\sum xy - (\sum x \sum y)}{\sqrt{\left[n\sum x^2 - (\sum x)^2\right]\left[n\sum y^2 - (\sum y)^2\right]}}, \tag{2.8}$$

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

Коефіцієнт кореляції, *r*, визначає, як силу, так і напрямок зв'язку між залежною і незалежною змінними. Значення *r* знаходяться в діапазоні від – 1.0 (сильний негативний зв'язок) до + 1,0 (сильний позитивний зв'язок). При *r* = 0 між змінними *x* і *y* немає ніякого зв'язку.

Розрахунок коефіцієнтів кореляції виконаний для кожного експерта окремо, тобто розраховувався за даними, наведеними у стовпцях табл. 2.4. Всього можливо три комбінації: МАІ – ранжування, МАІ – пряма розстановка, ранжування – пряма розстановка.

Результати розрахунків зображені на рис. 2.1. Оскільки графіки вагових коефіцієнтів частково пересікаються, то ступінь близькості методів визначався за середнім коефіцієнтом кореляції для кожного порівнюваного випадку.

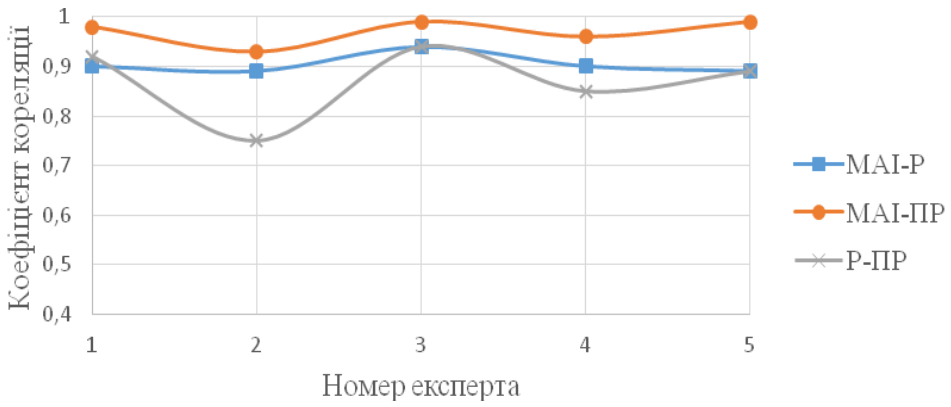


Рис. 2.1. Значення коефіцієнтів кореляції вагових коефіцієнтів за п’ятьма експертами

Найменше розходження виявилося у МАІ та прямої розстановки: середній коефіцієнт кореляції дуже високий і дорівнює 0,97. Це насамперед пов’язане з високою кваліфікацією експертів, а також фактом того, що експерти порівнювали фактори на протязі одного опитування та мали можливість корегувати свої результати, порівнюючи переваги одних факторів над іншими і їхню відповідність присвоєним відсоткам. Якщо відбувалося протиріччя, наприклад порушувалося правило транзитивності, то була можливість змінити

розставлені відсотки чи співставлення. Але необхідно відзначити, що при збільшенні кількості факторів, що оцінюються, можливість вдало корегувати пріоритетність стає важчою.

Середній коефіцієнт кореляції між рангами та MAI, рангами та прямою розстановкою дещо менший – 0,9 і 0,87 відповідно. Це пов'язано не лише з індивідуальними особливостями експертів, а також з деякими закономірностями. Одна з причин розходжень була закладена вже умовами ранжування, коли вимагалося, щоб фактори були розставлені у суворій послідовності у порядку спадання їх важливості, в той час як в MAI і при прямій розстановці можливість рівності факторів допускалася. Взагалі умова суворого ранжування не є обов'язковою, і часто погоджуються з пропозиціями Д. Хіммельблау [84] та інших авторів давати середній рейтинг двом або декільком факторам, якщо експерти вважають їхній вклад рівним. Тому не можна виключати можливість, що при умовах можливості надавати двом і більше факторам рівних рангів, корельованість результатів була б вищою.

Величина розходжень неоднакова у різних експертів і змінюється від 1% до 25%. Однак, як видно з рис. 2.1, тенденція корельованості результатів практично у всіх експертів однакова. Слід відзначити, що квазіпаралельний характер графіків кореляційних кривих дає підставу вважати, що логіка мислення експертів достатньо стійка і отримані в ході цього експерименту результати цілком можливо використовувати для досліджень.

2.1.3. Обробка експертних суджень

Знайдені в результаті обробки індивідуальних експертних суджень вагові коефіцієнти (табл. 2.3), необхідно усереднити. Задача полягає у знаходженні усереднених оцінок вагових коефіцієнтів для кожного фактору. Розв'язана вона може декількома способами.

Середнє арифметичне. Найпростішою оцінкою є середнє арифметичне по фактору:

$$\hat{k}_a = \frac{1}{m}\sum_{i=1}^{m} k_i \,, \tag{2.9}$$

де k_i – вага фактору *i*-го експерта.

Воно зручне тим, що після усереднення не порушується вимога рівності одиниці суми вагових коефіцієнтів. Усереднення проводиться для кожного фактору окремо. Таке усереднення допускається проводити у тих випадках, коли щільність розподілу k_i симетрична, наприклад, підлягає нормальному розподілу, або самі коефіцієнти практично однорідні і можуть бути апроксимовані рівномірним розподілом. Тоді оцінка $\hat{k}_a$ буде незміщеною.

Середнє геометричне. Вагові коефіцієнти за своєю природою не є лінійними. Тому для їх усереднення допустимо використовувати нелінійні методи. Одним з найпростіших методів нелінійної оцінки є середнє геометричне:

$$\hat{k}_{геом} = \sqrt[m]{k_1 k_2 \ldots k_m} \,. \tag{2.10}$$

Оскільки середнє геометричне завжди менше середнього арифметичного, сума усереднених вагових коефіцієнтів буде менше одиниці. Щоб цього не відбулося, необхідно кожний усереднений ваговий коефіцієнт $\hat{k}_{m.геом}$ нормувати на суму по всім факторам:

$$\hat{k}_{геом} = \frac{\hat{k}_{m.геом}}{\sum_{m=1}^{n} \hat{k}_{m.геом}} \,. \tag{2.11}$$

Середнє арифметичне і середнє геометричне мають один ліміт [84]. Отже, різниця між $\hat{k}_a$ та $\hat{k}_{геом}$ буде зменшуватися із збільшенням кількості експертів і

асимптотично наближатися до нуля.

Середнє гармонійне. Ще однією нелінійною величиною є середнє гармонійне. Його можна знайти з рівняння:

$$\frac{1}{\hat{k}_{гарм}} = \frac{1}{m}\sum_{i=1}^{m}\frac{1}{k_m}. \qquad (2.12)$$

Як відомо, середнє гармонійне менше середнього арифметичного і середнього геометричного. Отже, і вагові коефіцієнти, знайдені таким чином, також необхідно нормувати на суму коефіцієнтів усіх факторів за аналогією з формулою (2.11).

Медіана. Усереднення вагових коефіцієнтів також можливо провести за допомогою медіани. Особливо ефективно її використовувати для коротких рядів. Як відомо, медіана представляє собою найбільш ймовірні значення ряду:

$$\left.\begin{aligned} Me &= K_{\frac{n+1}{2}}, для\_непарних\_n, \\ Me &= \frac{1}{2}\left(K_{\frac{n}{2}+1} - K_{\frac{n}{2}} \right), для\_парних\_n, \end{aligned}\right\} \qquad (2.13)$$

де K_i – значення ваги фактору для i-го експерта.

При використанні медіани для усереднення в загальному випадку порушується виконуваність умови рівності одиниці сумі вагових коефіцієнтів. Тому необхідно здійснити відповідні нормування, щоб застосування вагових коефіцієнтів не втратило свій сенс.

Для дослідження залежності усереднених вагових коефіцієнтів від методу усереднення були проведені розрахунки за формулами (2.9 – 2.13). Виявилося, що метод усереднення слабо впливає на результуючі значення вагових коефіцієнтів – всі вони достатньо близькі між собою, що відображено на рис. 2.2.

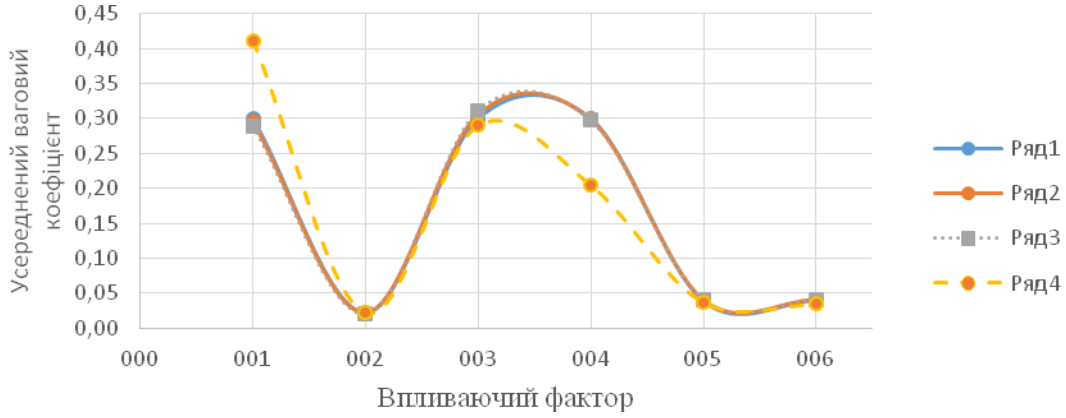


Рис. 2.2. Усереднені значення вагових коефіцієнтів впливаючих факторів (де ряд 1 – середнє арифметичне, ряд 2 – середнє геометричне, ряд 3 – середнє гармонійне, ряд 4 – медіана)

2.1.4. Переваги та недоліки MAI

Проаналізувавши основні підходи до формування КВ найбільш придатними для подальшого визначення впливовості критеріїв та проведення порівняльної характеристики стеганографічних методів був обраний метод аналізу ієрархій. У підсумку були визначені його переваги та недоліки саме для оцінки роботи методів вбудовування інформації у різних додатках.

Переваги методу.

На перший погляд, здається, що MAI являє собою ідеальний інструментарій для вирішення широкого кола багатофакторних задач, в яких експертні методи використовуються як ключові. Це багато в чому дійсно так, вкажемо на основні причини цього.

Попарність порівнянь. Порівняння предметів парами закладено в самій людській природі [49]. Відсутність необхідності постійно тримати у полі зору всі фактори або, принаймні, групу однорідних факторів, дозволяє експерту сконцентрувати увагу на конкретній проблемі: наскільки фактор A_i перевершує фактор B_j або поступається йому. Внаслідок цього слід очікувати більш точних

результатів.

Доповнюваність вихідної матриці. У практиці досліджень систем нерідко виникають ситуації, коли число факторів впливу змінюється. Тоді доводиться додавати, зменшувати або замінювати одні фактори іншими. При використанні МАІ частіше за все це призводить лише до необхідності порівняння новопосталих пар або ж до викреслювання рядків і стовпців матриці парних порівнянь, відповідних вилученим з розгляду факторам, тобто до утворення мінору матриці. Отримані результати попередніх опитувань зберігаються, і не потрібно повного оновлення анкети, як це відбувається в інших випадках. З урахуванням того, що процедура МАІ, по суті, зводиться до пошуку власного вектору відповідної матриці, що належить максимальному власному значенню, з «технічної» точки зору включення додаткових факторів є збільшення розмірності відповідного лінійного простору за рахунок додавання прямих доданків.

Наявність вербально-числової шкали. Звичайні числові шкали не завжди зручні для зіставлення факторів, які визначаються в різних розмірностях і поняттях. Особливо складно порівнювати чинники, характеристиками яких, з одного боку, є кількісні величини, а з іншого – якісні. Так, шкала Харрінгтона, що використовується найбільш часто, «приймає на вході» тільки відносні кількісні характеристики, розподілені в інтервалі від 0 до 1. Вербально-числові шкали, одним з варіантів яких є шкала Сааті, якраз і покликані оцінювати такі невідповідності показників факторів впливу.

Вбудований критерій якості роботи експерта. За результатами опитування експерти, як правило, підлягають перевірці. Для цього зазвичай застосовуються різні числові індекси, розроблені як для групових, так і для індивідуальних опитувань. При цьому питання про оптимальний критерій є відкритим, а його вибір довільний. У цьому сенсі наявність в МАІ такої характеристики (параметру), як відношення узгодженості, дуже зручне, особливо при створенні автоматизованого програмно-апаратного комплексу.

Недоліки методу.

Однак не всі переваги MAI так очевидні. Виникає ряд питань при інтерпретації результатів, і пов'язані вони, насамперед, з критерієм якості роботи експерта – з відношенням узгодженості.

Використання транзитивності для якісних показників. Транзитивність добре працює, коли всі характеристики системи, що досліджується, можна представити числовими величинами. Але як тільки це стає неможливим, вимога наявності транзитивності часто вступає у протиріччя з логікою дослідника.

«Зворотна» логіка. Критерії якості роботи експерта в своїй більшості, і відношення узгодженості також, ґрунтуються на відхиленні від якоїсь статистичної характеристики, наприклад, математичного сподівання. Як і всі критерії, що мають в основі статистичний характер, відношення узгодженості є формальним і в деяких випадках призводить до результатів, що достатньо важко інтерпретуються.

Аналізуючи результати опитувань експертів, які потрапляли в межі заданого рівня якості (ВУ < 10-20%), практично завжди виявляються випадки, коли деякі вагові коефіцієнти різко відрізняються від більшості, а то і носять прямо протилежний характер: фактори, яким більшість надавала найбільшу значимість, ці експерти оцінювали як менш значущі і – навпаки. При усереднені результатів всіх експертів, які відповідають заданому критерію, що зазвичай роблять для отримання узагальнених оцінок, це призводить до зміщення середніх значень вагових коефіцієнтів.

Ненадійність відношення узгодженості. Відношення узгодженості – формула (2.7) – засноване на порівнянні результатів даного експерта з якимось еталонним експертом – табл. 2.2. Однак, що таке еталонний експерт в MAI, не зовсім зрозуміло. Розглянемо ідеалізовану ситуацію, коли експерти розставляють оцінки, суворо дотримуючись транзитивності своїх переваг відносно нумерації факторів, тобто. $a_{ij} > a_{i+1,\,j+1}$ (або, навпаки, $a_{ij} < a_{i+1,\,j+1}$) – табл. 2.4.

Таблиця 2.4

Матриця парних порівнянь для восьми факторів

Фактори	Фактори								
	n	1	2	3	4	5	6	7	8
	1	1	8	8	8	8	8	8	8
	2	1/8	1	7	7	7	7	7	7
	3	1/8	1/7	1	6	6	6	6	6
	4	1/8	1/7	1/6	1	5	5	5	5
	5	1/8	1/7	1/6	1/5	1	4	4	4
	6	1/8	1/7	1/6	1/5	1/4	1	3	3
	7	1/8	1/7	1/6	1/5	1/4	1/3	1	2
	8	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1

Отримання результатів на основі такої матриці дає значення відношення узгодженості 23,3%. Для $n = 9$ при побудові такого ж типу матриці ВУ складе вже 27,8%, а зростання ВУ буде збільшуватися зі збільшенням числа факторів.

2.2. Синтез критерію для порівняння стеганографічних методів

Як було розглянуто вище, в сучасному світі існує багато областей застосування стеганографічних методів [85]. Кожен з цих 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 [86]. Необхідно визначити КВ критеріїв оцінки стеганографічних систем, наведених в п. 1.3.2, таких як пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення інформації [97].

2.2.1. Вимоги, що висуваються стеганографічними додатками

Найголовнішою вимогою до стеганографічних методів, що використовуються для створення *систем прихованого зв'язку*, є неможливість виявлення вбудованого повідомлення. Це означає, що зображення із та без секретного вкладення мають здаватися ідентичними при будь-яких можливих статистичних тестах, що можуть бути здійснені. Вкрай важливо знати якомога більше статистичних властивостей джерела, з якого береться зображення-контейнер. Наприклад, якщо стеганографічними контейнерами є скановані зображення, їм буде властива сильніша кореляція в горизонтальному напрямку, аніж у перпендикулярному. Характеристики шуму можуть бути специфічними для кожного окремого сканера і повинні бути прийняті до уваги, якщо потребується надійна, захищене стеганографічна система. З іншого боку, якщо зображення зняте за допомогою цифрової ПЗЗ камери, шум знову ж таки матиме специфічні властивості, викликані елементами ПЗЗ і особливостями зчитування даних. У кожному разі, алгоритм приховування даних повинен відповідати всім відомим статистичним властивостям джерела зображення і отримане зображення із секретним повідомленням не може бути відрізнене від знімків, які не містять будь-яких вкладень.

Іншою важливою вимогою є пропускна здатність каналу зв'язку. Зрозуміло, що можна вбудувати один біт інформації в кожен кадр відео послідовності, і не враховувати завадову обстановку. Однак, така система зв'язку призведе до неефективно низької пропускної здатності каналу. Завдання полягає в тому, щоб вбудувати якомога більше інформації, не порушуючи існуючу модель шуму зображення.

Останньою важливою вимогою є можливість вилучення прихованого повідомлення без наявності оригінального зображення. Іноді це може бути вирішене заздалегідь узгодженою базою зображень, що одноразово

використовуються в якості контейнера. Але це суттєво обмежує можливість застосування такого методу.

Вимогою до методів вбудовування ЦВЗ з метою *захисту авторських прав та автентифікації* є надійність, захищеність, невидимість, а також незворотність його накладання на вихідне зображення (для запобігання IBM атак). Методи ЦВЗ можуть використовувати вихідне зображення для вилучення цифрової мітки. Це спрощує детектування зображення-контейнеру перед його декодуванням. Іншою особливістю є порівняно невелика пропускна здатність (1-100 біт).

Вбудовування ідентифікаційних номерів («відбитки пальців») потребує алгоритму, що би незворотнім чином накладав стійкий, захищений, невидимий ЦВЗ на вихідне зображення. Методи ЦВЗ в даному випадку не повинні використовувати оригінал зображення для вилучення мітки. Оскільки є можливість, що велика кількість документів, позазначених різними мітками, будуть розподілені у загальне користування, методи мають бути стійкими до атак змови. До інших особливостей відноситься порівняно невелика пропускна здатність.

Для збереження якості контейнеру, в який *вбудовується заголовок або інша додаткова інформація* стеганографічний метод має забезпечувати достатню стійкість до стиснення із втратами та додавання шуму, а також невидимість водяного знаку, навіть великого обсягу. Вихідні зображення (кадри) в даному випадку не доступні для процесу вилучення повідомлень. Оскільки прихована інформація є корисною для споживача, немає необхідності вимагати захищеності – споживач не зацікавлений у видаленні вкладених даних. Зважаючи на те, що водяний знак має бути відновлений у реальному часі, є необхідність у високій швидкості вилучення повідомлення. Але з іншого боку, процес вбудовування ЦВЗ може бути більш трудомістким.

Для програмного забезпечення, що може бути використано *для захисту цілісності зображення*, наприклад, Adobe PhotoShop або PaintShop Pro,

важливим є забезпечення стійкості, захищеності та невидимості вбудованого ЦВЗ. В таких додатках детектор працює без наявності вихідних зображень.

Для управління копіюванням при DVD записі необхідно мати можливість вбудувати у кадр стійкий, прозорий, захищений ЦВЗ. Оригінальні кадри зазвичай недоступні для вилучення мітки.

Для використання стеганографії *в інтелектуальних браузерах* та *для автоматичного надання інформації про авторські права* необхідно забезпечити стійкість, невидимість та захищеність відкритого детектору, що реалізований у програмному забезпеченні. На даний час точно не відомо, чи існує захищений відкритий детектор у ПО взагалі.

У роботі [24] було проведене детальне дослідження та оцінені вимоги до характеристик окремо для кожної з розповсюджених стеганографічних сфер застосування за кольоровою шкалою (рис. 2.3).

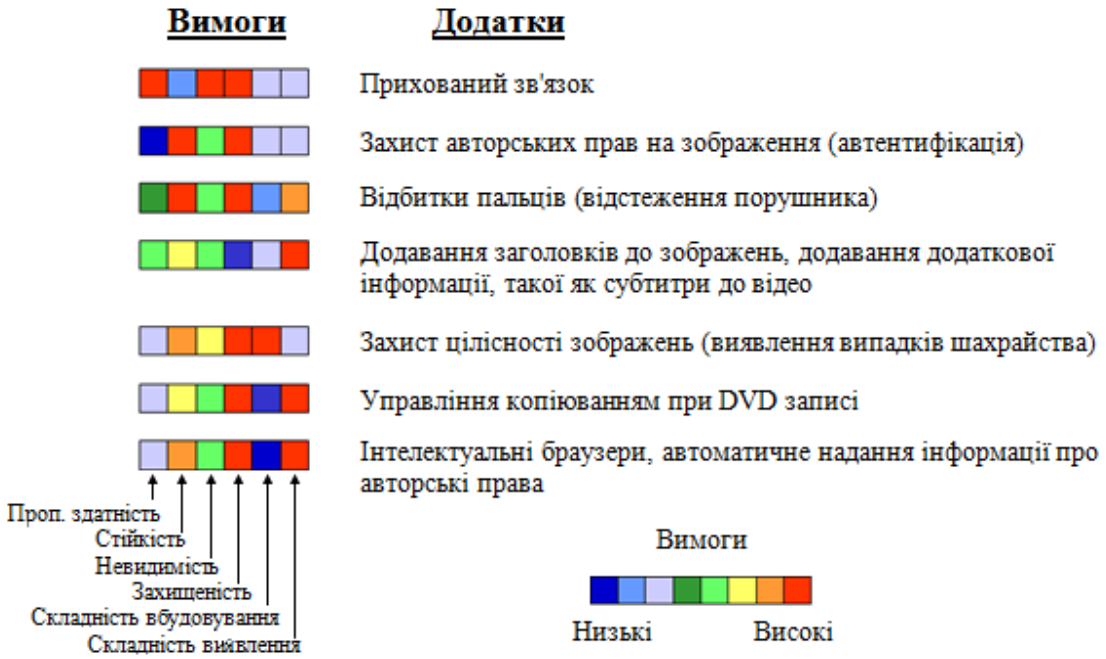


Рис. 2.3. Основні сфери використання та їх вимоги до характеристик

Використовуючи набір характеристик, запропонованих у п. 1.3.2 пропонується провести попарне порівняння показників методом аналізу ієрархій для кожного з додатків.

2.2.2. Розрахунок ваг характеристик

Формою представлення попарних порівнянь [43] є зворотно-симетрична матриця (табл. 2.6), елементи якої W_{ij} є проявами інтенсивності елементів ієрархії *i* відносно ієрархії *j*, що оцінюється за шкалою інтенсивності від 1 до 9, де оцінки мають наступні значення:

1 – рівні значення;

3 – помірна перевага одного над іншим;

5 – істотна перевага одного над іншим;

7 – значна перевага одного над іншим;

9 – дуже сильна перевага одного над іншим;

2, 4, 6, 8 – відповідні проміжні значення.

Для отримання матриці парних співставлень (табл. 2.6) була запропонована матриця (табл. 2.5), що перетворює кольори у коефіцієнти від 1 до 9.

Таблиця 2.5

Матриця відповідності

	1	1/2	1/3	1/4	1/5	1/6	1/7	1/9
	2	1	1/2	1/3	1/4	1/5	1/6	1/7
	3	2	1	1/2	1/3	1/4	1/5	1/6
	4	3	2	1	1/2	1/3	1/4	1/5
	5	4	3	2	1	1/2	1/3	1/4
	6	5	4	3	2	1	1/2	1/3
	7	6	5	4	3	2	1	1/2
	9	7	6	5	4	3	2	1

Після цього були побудовані матриці пріоритетів (табл. 2.6, табл. 2.7, Додаток В), що включають: пропускну здатність (*a*), стійкість (*b*), невидимість (*c*), захищеність (*d*), складність вбудовування (*e*) і складність вилучення (*f*).

Таблиця 2.6

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	

Таблиця 2.7

Матриця пріоритетів (для додатку орієнтованого на захист цілісності зображення)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/5	1/4	1/6	1/6	1
b	5		2	1/2	1/2	5
c	4	1/2		1/3	1/3	4
d	6	2	3		1	6
e	6	2	3	1		6
f	1	1/5	1/4	1/6	1/6	

При заповненні матриць пріоритетів керуються правилом: якщо при порівнянні елемента *i* з елементом *j* отримано $W_{ij} = b$, тоді $W_{ij} = 1/b$.

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

Точне визначення основних пріоритетів власного вектора матриці є досить складним. На практиці [43] запропоновано використовувати один із таких способів:

1. Підсумовуються елементи кожного рядка і нормуються шляхом ділення отриманої суми на суму всіх елементів матриці. Перший елемент отриманого вектора буде пріоритетом першого об'єкта, другий другого і т.д.

2. Підсумовуються елементи кожного стовпця і знаходяться обернені величини цих сум. Вони нормуються шляхом поділу кожного на обернену величину їх загальної суми, таким чином що загальна сума нормованих величин дорівнюватиме одиниці.

3. Елементи кожного стовпця діляться на суму елементів цього стовпця (нормується стовпець), потім отримані елементи кожного з рядків сумуються і діляться на кількість елементів у рядку.

4. Розраховується середнє геометричне кожного рядка, і отримані значення нормуються.

5. Матриця підноситься до як завгодно великого ступеню, обчислюється сума елементів рядків і отримані величини нормуються.

Був використаний спосіб, орієнтований на розрахунок середнього геометричного кожного рядка (4), згідно з яким компоненти вектора пріоритетів обчислюються таким чином:

$$V_i = \frac{\sqrt[N]{\prod_{j=1}^{N} W_{ij}}}{\sum_{k=1}^{N} \sqrt[N]{\prod_{j=1}^{N} W_{kj}}}, \qquad (2.14)$$

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

Шляхом усереднення результатів для всіх додатків (2.15) отримуємо ваги (важливість) кожної з характеристик стеганографічних методів (табл. 2.8).

$$R_i = \sum_{i=1}^{7} V_i / 7. \qquad (2.15)$$

Таблиця 2.8

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).

2.3. Порівняльний аналіз методів за синтезованим і існуючими критеріями

Отримані оцінки використовуються для аналізу обраних стеганографічних методів вбудовування інформації та для багатокритеріального вибору найкращого методу. На основі інформації, представленій в [25, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 97], та використовуючи метод присвоєння коефіцієнтів факторам, була створена табл. 2.9, де:

A1 – метод заміни найменш значущих біт (НЗБ) [22, 25];

A2 – метод Куттера-Джордана-Боссена [25, 34];

A3 – метод Коха-Жао [25, 35];

A4 – метод Бенгама-Мемона-Ео-Юнга [25, 36];

A5 – метод із розширенням спектру [40, 41, 42, 93, 94];

A6 – метод, заснований на 3-рівневому ДВП [44, 89, 90, 91, 92].

Таблиця 2.9

Порівняльний аналіз методів вбудовування

	a	*b*	*c*	*d*	*e*	*f*
A1	8	1	7	1	8	8
A2	6	4	7	4	7	7
A3	2	7	5	7	5	5
A4	1	6	6	7	4	4
A5	4	7	8	6	3	3
A6	3	8	8	8	1	1

Де: *a* – пропускна здатність; *b* – стійкість; *c* – невидимість; *d* – захищеність; *e* – складність вбудовування; *f* – складність виявлення.

У табл. 2.9 показник «8» є кращим значенням характеристики, «1» – найгіршим. Для розуміння значень, що описані в табл. 2.9, нижче наведений розрахунок коефіцієнтів для пропускної здатності.

Для методу НЗБ пропускна здатність залежить від розмірів зображення (*h* – висота, *w* – ширина) і розраховується згідно з:

$$C_1 = h \cdot w \cdot 3. \qquad (2.16)$$

Зазвичай тільки один колірний компонент використовується для приховання, але можливість вбудувати інформацію є одразу у всі (три) компоненти.

У методі Куттера один біт інформації може бути вбудований в один піксель зображення, таким чином пропускна здатність визначається як:

$$C_2 = h \cdot w. \tag{2.17}$$

Метод Коха-Жао використовує для вбудовування одного біту інформації блок коефіцієнтів ДКП розміром *8x8*, тому пропускна здатність визначається:

$$C_3 = (h \cdot w) / (8 \cdot 8) \tag{2.18}$$

В методі Бенгама блоки діляться на три класи, і тільки один може бути використаний для вбудовування, так чином в середньому:

$$C_4 = (h \cdot w) / (8 \cdot 8 \cdot 3). \tag{2.19}$$

Для методів розширення спектру пропускна здатність визначається за формулою Шеннона:

$$C_5 = B \cdot \log_2(1 + SNR), \tag{2.20}$$

де $B = h \cdot w$.

Після визначення допустимого рівня відношення сигнал/шум (*SNR*) можна подати вираз (2.20) у вигляді:

$$C_5 = h \cdot w \cdot 0.264. \tag{2.21}$$

Методи, що використовують ДВП перетворення першого рівня, можуть запропонувати пропускну здатність:

$$C_6 = (h \cdot w) / 4. \qquad (2.22)$$

Після розрахунку середніх значень (2.16) – (2.22) були визначені коефіцієнти пропускної здатності (перша колонка в табл. 2.9) шляхом прямої розстановки методів.

Щодо інших характеристик, то стійкість була оцінена через кількість загальних операцій з обробки зображення, які можливо здійснити зі стеганографічною системою, утвореною певним методом, без втрати можливості детектувати вбудовану інформацію [40]. Невидимість оцінювалася кількісним показником якості зображення (*IF*). Захищеність оцінювалася на основі даних вказаних в публікаціях [24, 80, 81, 82, 83] і враховувала стійкість методів до атак. Складність вбудовування і вилучення розраховувалася за кількістю стандартних операцій, які необхідно виконати для вбудовування і вилучення прихованого повідомлення. При цьому стеганографічний контейнер заповнювався лише на 10% від максимальної пропускної здатності.

Отже, на основі даних, наведених у табл. 2.9 можна провести комплексний порівняльний аналіз обраних методів *A1* – *A6*. Для цього використовується методика попарних порівнянь, описана у п. 2.2.2. Порівняльний аналіз методів, заснований на детальному аналізі кожної з характеристик, відображений у вигляді матриць в табл. 2.10, табл. 2.11. та Додатку Г.

Таблиця 2.10

Матриця порівняння методів (за пропускною здатністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		3	7	8	5	6
A2	1/3		5	6	3	4
A3	1/7	1/5		2	1/3	1/2
A4	1/8	1/6	1/2		1/4	1/3
A5	1/5	1/3	3	4		2
A6	1/6	1/4	2	3	1/2	

Таблиця 2.11

Матриця порівняння методів (за захищеністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		1/4	1/7	1/7	1/6	1/8
A2	4		1/4	1/4	1/3	1/5
A3	7	4		1	2	1/2
A4	7	4	1		2	1/2
A5	6	3	1/2	1/2		1/3
A6	8	5	2	2	3	

Оцінки методів *A1 – A6* по окремим характеристикам були отримані за формулою (2.14). Підсумовуючи значення всіх параметрів (2.23) та віднормувавши їх, виходять параметри зваженої оцінки якості методів, що наведені в табл. 2.12.

$$WW_a = \frac{\sum_{i=1}^{k=6} V_i}{\sum_{a=1}^{A=6}\sum_{i=1}^{k=6} V_{ia}}, \qquad (2.23)$$

де $k = 6$ – кількість характеристик;

A – кількість методів;

V_i – вектор пріоритетів по кожній з характеристик, який розраховується з (2.14);

V_{ia} – вектор пріоритетів по кожній з характеристик a для кожного з методів. Найбільші значення в табл. 2.12 та табл. 2.13 є найліпшими.

Таблиця 2.12

Порівняння методів, не враховуючи важливість (вагу) характеристик

Метод (a)	Значення (WW)
A1	0,266
A2	0,181
A3	0,126
A4	0,097
A5	0,137
A6	0,193

Як видно з табл. 2.12, найвище значення продемонстрував метод НЗБ (*A1*, $WW = 0{,}266$). Але зважаючи на оцінку важливості характеристик табл. 2.12 може бути видозмінена до табл. 2.13, де значення параметрів були отримані з виразу (2.24):

$$WW1_a = \frac{\sum_{i=1}^{k=6}(V_i \cdot R_i)}{\sum_{a=1}^{A=6}\sum_{i=1}^{k=6} V_{ia} \cdot R_i}, \qquad (2.24)$$

Таблиця 2.13

Порівняння методів, враховуючи важливість (вагу) характеристик

Метод (*a*)	Значення (*WW1*)
A1	0,081
A2	0,086
A3	0,184
A4	0,146
A5	0,170
A6	0,333

Таким чином, при комплексному порівнянні методів вбудовування інформації для використання у стеганографічних додатках при передачі по мережах зв'язку, найкращий результат показали інтегровані методи, засновані на ДВП (*A6*, *WW1* = 0,333) та дискретному косинусному перетворенні (ДКП) (*A3*, *WW1* = 0,184).

2.4. Висновки до другого розділу

У другому розділі дисертаційної роботи були отримані наступні результати:

1. Обрано математичний апарат для багатокритеріальної оптимізації. Визначено найбільш придатний метод багатокритеріальної оцінки для експертного оцінювання стеганографічних методів та характеристик, а саме метод аналізу ієрархій.

2. Підтверджено можливість використання результатів оцінок експертів у подальших дослідженнях. Оскільки графіки кореляційних кривих оцінок експертів за принципом ранжування факторів, прямої розстановки та методу аналізу ієрархій мають квазіпаралельний характер, що дає підставу вважати логіку мислення експертів стійкою.

3. Встановлено, що процедура усереднення не грає суттєвої ролі для визначення вагових коефіцієнтів, принаймні, для отриманих у поточній роботі даних експертних суджень. Оскільки усереднення вагових коефіцієнтів шляхом розрахунку середнього арифметичного, середнього геометричного, середнього гармонічного та медіанних оцінок, при умові нормування трьох останніх характеристик, показало, що отримані таким чином, значення близькі між собою.

4. 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.

5. На основі комплексного критерію оцінювання стеганографічних систем передачі інформації були визначені оптимальні методи приховування інформації в разі присутності активного порушника. Найліпші результати показують методи, засновані на ДВП (*А6*, метрика *WW1* = 0,333) та ДКП (*А3*, метрика *WW1* = 0,184).

РОЗДІЛ 3
АНАЛІЗ СТІЙКОСТІ МЕТОДІВ НА ТЛІ ЗОВНІШНІХ ВПЛИВІВ

Всі сфери застосування стеганографічних методів, що розглянуті у п. 1.1, в тій чи іншій мірі використовують математичну модель, схематично зображену на рис. 1.6. При передачі по каналах зв’язку заповнене зображення-контейнер з великою ймовірністю піддається атакам або підпадає під вплив завад.

Завади – сигнали або дії, що спотворюють корисний сигнал, який несе основну інформацію у пристроях зв'язку. Вплив завади може призвести до значних помилок у стеганографічній системі [95].

Атаки – це будь-яка спроба детектувати, вилучити, змінити приховане стеганографічне повідомлення [96].

Одні стеганографічні додатки частіше потерпають від завад у каналах звя’зку, наприклад, стеганосистеми прихованого зв’язку та системи захисту прав на зображення. Інші постійно піддаються атакам з боку користувачів, особливо при використання стеганографіїї з метою відстеження порушника або виявлення випадків неліцензійного тиражування та шахрайства.

Здатність стеганографічних систем протистояти атакам та завадам називається *стійкістю* або *захищеністю*, в залежності від умов та мети впливів [24].

3.1. Оцінювання стійкості до навмисних атак

Як відомо, основним завданням стеганографії є приховання самої наявності стеганографічного каналу. Але у випадку зловмисних дій порушник може припускати його наявність і застосовувати до зображення різні атаки з метою руйнування або видалення вбудованих даних. У той же час, повноправний користувач, не знаючи про наявність прихованої інформації, також може здійснювати атаки на ЦВЗ, не усвідомлюючи цього.

Найпростішою атакою є суб'єктивна (візуальна), коли зловмисник уважно розглядає зображення, намагаючись визначити «на око», чи є в ньому приховане повідомлення. Подібна атака може бути дієвою лише проти абсолютно незахищених стеганосистем. Тим не менш, вона є найпоширенішою на початковому етапі розкриття стеганографічної системи. Візуальну непомітність вкладення при оцінюванні методу вбудовування характеризує параметр *невидимості* [22].

3.1.1. Класифікація атак на стеганографічні системи

Існує безліч класифікацій атак на стеганографічні системи, але загалом їх можна поділити на [22]:

1. Атаки проти вбудованого повідомлення – направлені на видалення чи псування ЦВЗ шляхом маніпулювання стеганоконтейнером. Виділяють наступні види даних атак: стиснення зображення, додавання шуму, зміна контрастності, застосування лінійних і нелінійних фільтрів (розмитість, підвищення різкості, медіанна фільтрація).

2. Атаки проти стеганодетектора – направлені на те, щоб зробити важким, або неможливим правильну роботу детектора. При цьому водяний знак в зображенні залишається, але губиться можливість його прийому. Виділяють такі атаки, як афінні перетворення (тобто, масштабування, зсуви, повороти), відсічення зображення, перестановка пікселів, друку/копіювання/сканування, квантування кольорів тощо.

3. Атаки проти протоколу вбудовування повідомлення – в основному пов'язані зі створенням помилкових вкладень та ЦВЗ, інверсією водяних знаків, додаванням кількох ЦВЗ, тощо.

4. Атаки проти самого водяного знаку – спрямовані на оцінювання та вилучення ЦВЗ із стеганосистеми, по можливості без спотворення контейнера. У цю групу входять такі атаки, як атаки змови, статистичного

усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації та інші.

Наймасовішими атаками, яким піддаються стеганографічні системи є перші два типи (рис. 3.1).

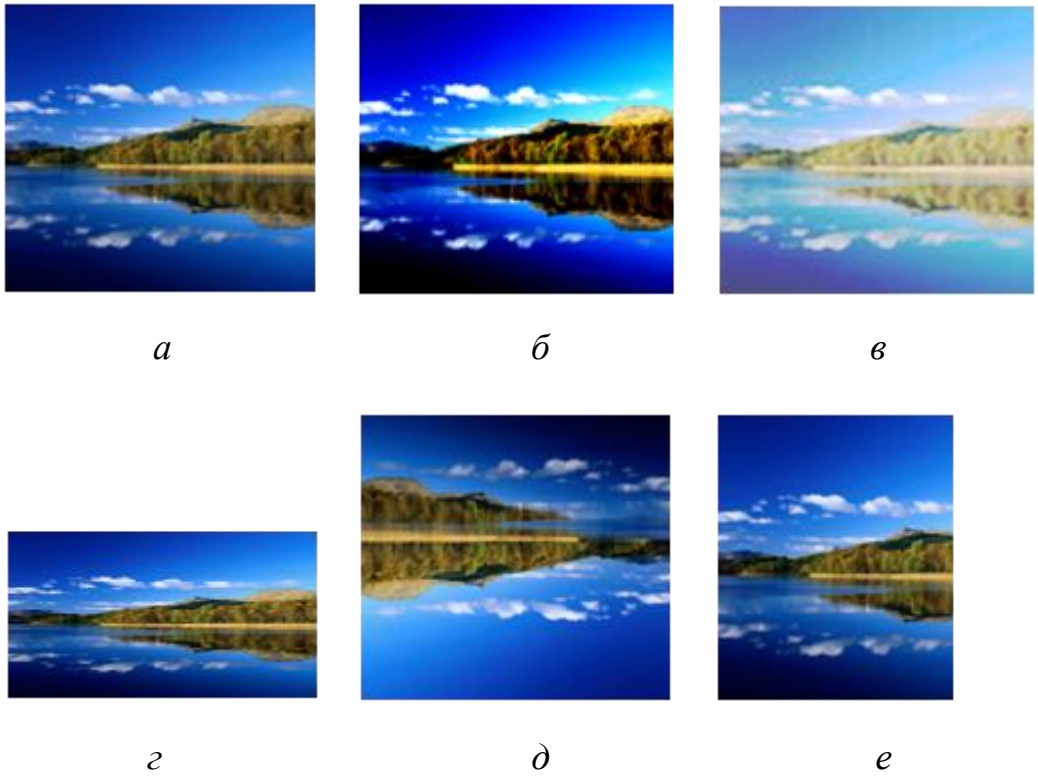


Рис. 3.1. Реалізація атак на вбудоване повідомлення і стеганодетектор (*а* – оригінальне зображення, *б* – зміна контрастності, *в* – зміна яскравості, *г* – масштабування, *д* – поворот, *е* – відсічення)

3.1.2. Дослідження стійкості стеганографічних систем до атак

Для дослідження впливу атак проти стеганографічного детектора (рис. 1.6) розглядаються геометричні атаки, тому що саме їх найчастіше застосовують до зображень середньостатистичні користувачі, переслідуючи особисті цілі. Геометричні атаки математично моделюються як афінні перетворення невідомі детектору. Вони призводять до втрати

синхронізації в детекторі, при цьому водяний знак у зображенні залишається, але втрачається можливість правильного його детектування [98].

Результати геометричних впливів на здатність правильного детектування ЦВЗ наведені в табл. 3.1, де тут і в подальшому НЗБ – метод заміни найменш значущого біта, КДБ – метод Кутера-Джордана-Боссена, КЖ – метод Коха-Жао, БМЕЮ – метод Бенгама-Мемона-Ео-Юнга, ДВП – метод на основі вейвлет-перетворення. У відсотках вказана максимально допустима величина змін. Реалізація атак здійснювалася за допомогою програмних засобів Adobe Photoshop і Microsoft Office Picture Manager.

Таблиця 3.1

Аналіз стійкості до атак проти стеганографічного детектора

Вид геометричної атаки	в просторовій обл.		в частотній обл.		в обл. перетв.
	НЗБ	КДБ	КЖ	БМЕЮ	ДВП
1. Масштабування	–	–	–	–	–
2. Зміна пропорцій	–	17%	1%	–	–
3. Повороти	–	–	–	–	+
4. Відсічення	–	–	–	–	+
6. Яскравість	–	17%	18%	15%	20%
7. Контрастність	–	52%	55%	5%	60%

Після аналізу зображень (рис. 3.1, а), зробимо висновок, що атаки проти стеганодетектора засновані на масштабуванні, повороті і відсіченні зображення (рис. 3.1 г, д, е) призводять до не спрацювання детектора. Жоден з досліджуваних методів не виявив до них стійкості.

В якості найімовірніших атак проти вбудованого повідомлення були обрані: переформатування і стиснення зображення з вкладеним ЦВЗ (табл. 3.2).

Де у відсотках вказаний ступінь компресії зображення при переформатуванні зображення у формат *JPG*.

Таблиця 3.2

Аналіз стійкості до атак проти вбудованого повідомлення

Переформатув. / стиснення	в простор. обл.		в частотній обл.				в обл. перет.
	НЗБ	КДБ	КЖ		БМЕЮ		ДВП
Розмір зображення:	640× 640	640× 640	2048× 2048	640× 640	2048× 2048	640× 640	640× 640
bmp-png	+	+	+	+	+	+	+
bmp-tiff	+	+	+	+	+	+	+
bmp-jpeg(rgb)/0%	–	–	+	+	+	+	+
bmp-jpeg(rgb)/25%	–	–	+	+	+	+	+
bmp-jpeg(rgb)/50%	–	–	+	+	+	+	+
bmp-jpeg (Ycbcr)/0%	–	–	+	–	+	–	+
bmp-jpeg (Ycbcr)/25%	–	–	+	–	–	–	+
bmp-jpeg (CMYK)/0%	–	+	+	+	+	+	+
bmp-jpeg (CMYK)/25%	–	–	+	+	+	+	+

Таким чином, найвищий рівень стійкості та захищеності до стеганографічних атак серед методів вбудовування у просторову область показав метод Куттера-Джордана-Боссена. Але навіть він значно програє

методам, що використовують область перетворення, при дослідженні впливів атак проти вбудованого повідомлення.

Дослідження показали, що найефективнішим способом приховування даних є вейвлет-перетворення. Їх використання є доцільним при наявності активного порушника, навіть у вигляді законного власника. Метод виявився найбільш стійким до геометричних атак, а також продемонстрував відмінні характеристики при стисненні зображень. Єдиною вимогою є правильний вибір діапазону частот для вбудовування, що визначає стійкість зображення до стиснення.

3.2. Оцінювання стійкості до завад у каналах зв'язку

Для того, щоб оцінити можливість методів адаптуватись до реальних каналів зв'язку, був створений програмний комплекс, що імітує обрані канали. Після накладання певних завад оцінювалися порогові значення спотворень, для яких ще можливе відновлення прихованої інформації.

Для досліджень було обрано наступні канали зв'язку:

1. Канал із адитивним білим гаусовим шумом (АБГШ) – найпростіший математичний канал телекомунікаційного зв'язку. В цій моделі корисний сигнал $s(t)$ спотворюється адитивним випадковим шумом $n(t)$ (рис. 3.2).

$$Z(t) = \gamma u(t-\tau) + n(t) = s(t) + n(t), \tag{3.1}$$

де $n(t)$ – адитивний гаусів шум із нульовим математичним очікуванням та заданою кореляційною функцією. Часто при аналізі можна не враховувати τ, що відповідає зміні початку відліку часу на виході каналу.

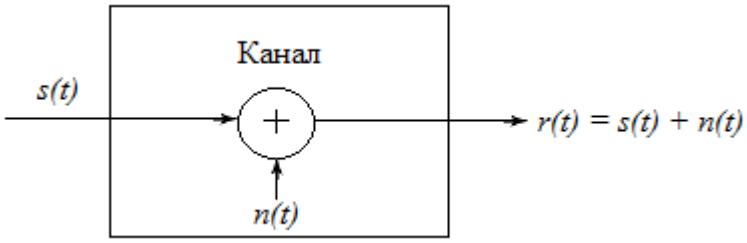


Рис. 3.2. Модель каналу із адитивним білим гаусовим шумом

Дана модель вдало описує багато провідних каналів, радіоканалів при зв'язку у прямій видимості, а також радіоканали з повільними загальними завмираннями, при яких можна точно передбачити значення γ та τ. Адитивний шум може збільшуватися із-за електричних компонентів і підсилювачів приймача комунікаційної системи, або із-за інтерференцій, що зустрічаються при передачі, особливо радіосигналів [99].

2. Канал із мультиплікативною завадою, що описується як дискретний симетричний канал без пам'яті, у якому кожен переданий символ може бути прийнятий помилково із фіксованою ймовірністю $P_{помилки}$ та вірно із ймовірністю $1 - P_{помилки}$. Ймовірність помилкового прийому не залежить від передісторії передачі [100].

Мультиплікативні завади обумовлені сторонньою зміною коефіцієнта передачі каналу зв'язку (рис. 3.3).

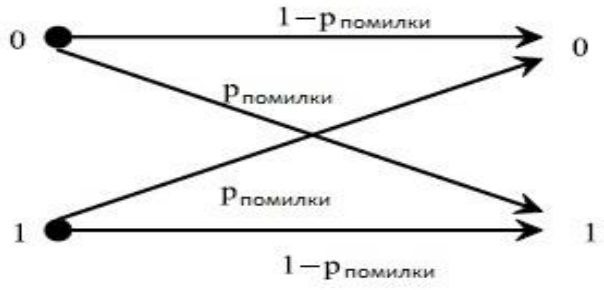


Рис. 3.3. Модель каналу з мультиплікативною завадою

3. Двійковий канал із стиранням, який працює так, що кожен переданий біт або правильно прийнятий без помилок, або повністю втрачений з ймовірністю $P_{стирання}$. Під цим розуміють прийом замість «1» або «0» якогось третього символу (символу стирання), що вказує на позицію спотвореного символу (рис. 3.4).

Такий канал зустрічається в сучасних мережах з комутацією пакетів, високошвидкісних каналах супутникового зв'язку, тощо.

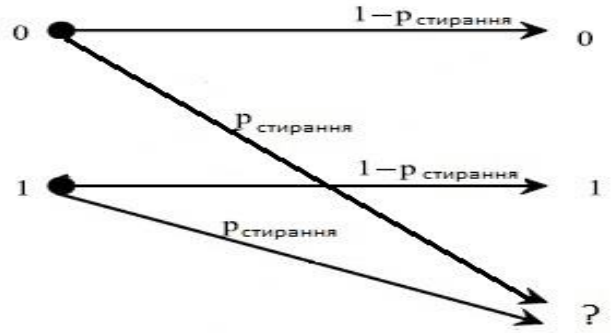


Рис. 3.4. Модель каналу зі стираннями

Розроблений програмний комплекс дозволяє працювати із двома типами файлів (*bmp* та *txt*) та трьома моделями каналу зв'язку. При цьому кожен файл подається в бінарному коді, отже канал впливає на інформацію побітово [99, 100].

Основними результатами є отримані порогові значення спотворень, для яких ще можливе відновлення прихованої інформації (табл. 3.3).

Таблиця 3.3

Порогові значення спотворень контейнера для відновлення інформації

Метод	Канал з АБГШ, $\sigma_{завади}^2$	Канал із мультиплікативною завадою, $P_{помилки}$, %	Канал із стираннями, $P_{стирання}$, %
A1	0,2	1	1
A2	0,2	1	1
A3	0,2	0,3	0,3
A4	0,2	0,03	0,03
A6	0,2	0,5	0,5

Також були розраховані кількісні показники для оцінки методів, що досліджуються. На рис. 3.5 та рис. 3.6 представлені графіки усереднених характеристик *SNR* та *NAD* на порогових значеннях спотворень контейнерів. Тобто по осі ординат відкладені мінімальні значення *SNR* для кожного з методів, при якому можливе правильне вилучення прихованої інформації (рис. 3.5), і максимальні показники *NAD* відповідно (рис. 3.6).

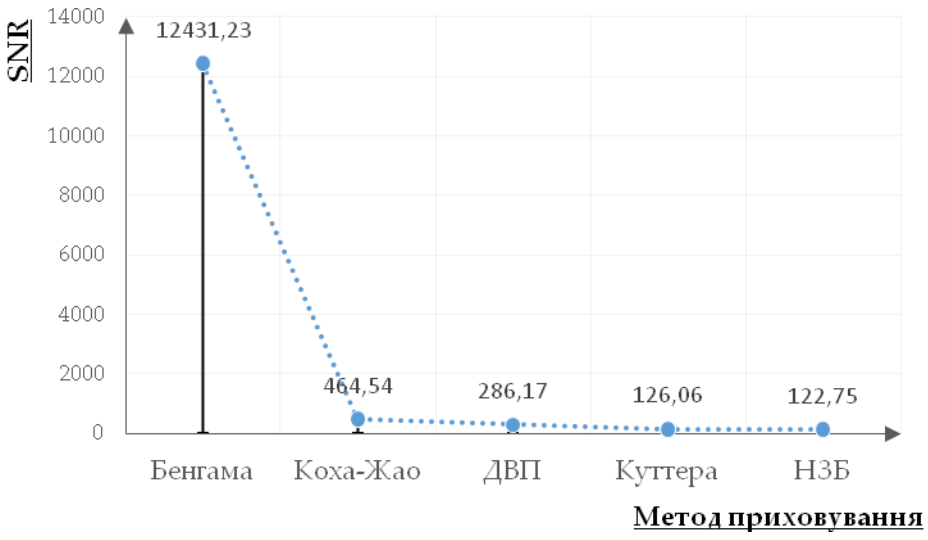


Рис. 3.5. *SNR* для порогових значень спотворень для кожного з методів

Отже, найменшого рівня *SNR* для вилучення вбудованого повідомлення після передачі у каналі зв’язку із завадами потребують стеганографічні методи, що використовують просторову область зображення.

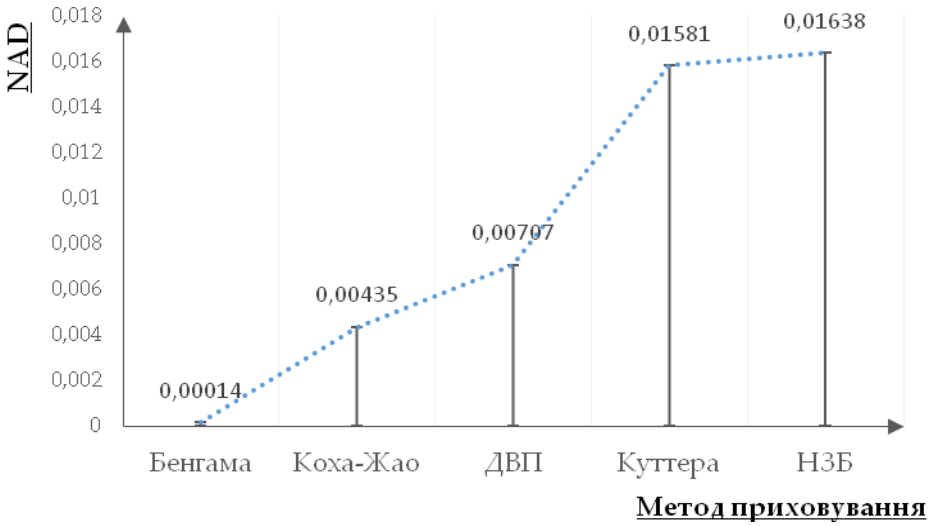


Рис. 3.6. *NAD* для порогових значень спотворень для кожного з методів

Вимоги до співвідношення сигнал/шум (*SNR*) збільшуються із збільшенням складності реалізації методу вбудовування, а нормована середня абсолютна різниця має обернено-пропорційний зв’язок.

Загалом найпростіші методи, що оперують із просторовою областю зображення, виявилися найбільш стійкими до обраних завад у комунікаційних каналах. Метод дискретного вейвлет-перетворення показав значення на рівні найкращих. В той час, як частотні методи потребують значно вищого рівня *SNR* для детектування прихованого повідомлення, та мають нижчі граничні показники допустимих спотворень.

3.3. Аналіз методів підвищення стійкості до зовнішніх впливів

3.3.1. Аналіз методів підвищення стійкості до атак

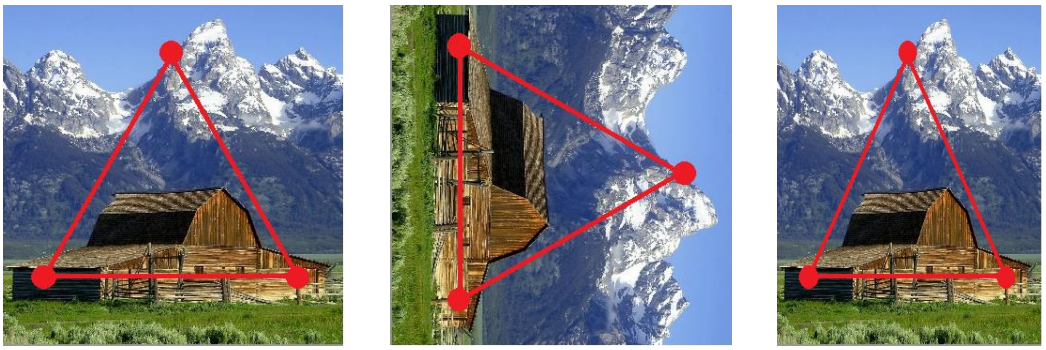
Найпоширенішими атаками на стеганографічні системи є геометричні атаки. Вони, на відміну від атак видалення, прагнуть змінити ЦВЗ шляхом внесення просторових або часових спотворень. Геометричні атаки математично моделюються як афінні перетворення з невідомим декодеру параметром. В загальному випадку є шість афінних перетворень: масштабування, зміна пропорцій, повороти, зсуви та відсічення. Ці атаки призводять до втрати синхронізації в детекторі ЦВЗ і можуть бути локальними або глобальними (тобто застосованими до всього сигналу). При цьому можливе вирізання окремих пікселів або рядків, перестановка їх місцями, застосування якихось перетворень і т. і. Подібні атаки реалізовані в програмах Unsign (локальні атаки) і Stirmark (локальні і глобальні атаки).

Існують і більш «інтелектуальні» атаки, що базуються на методі синхронізації ЦВЗ. Основна ідея цих атак полягає в розпізнаванні методу синхронізації та руйнації його шляхом згладжування піків в амплітудному спектрі ЦВЗ. Атаки ефективні в припущенні про те, що в якості механізму синхронізації використовуються періодичні шаблони. При цьому для забезпечення синхронізації можуть використовуватися два підходи: вбудовування піків в спектральній області, або періодичне впровадження послідовності ЦВЗ. В обох випадках в спектрі утворюються піки, які руйнуються в розглянутій атаці. Після руйнування можна застосовувати інші геометричні атаки: синхронізації вже немає [101].

Важливе значення має розробка систем із водяними знаками, що можуть витримати геометричні спотворення, а також зміну значень пікселів. Великий акцент робиться на стійкість водяних знаків до спотворення величини пікселів в результаті стиснення і фільтрації сигналу. Нажаль, дослідження останніх

часів демонструють, що навіть невеликі геометричні перетворення можуть зруйнувати водяний знак [102]. Ця проблема постає найгостріше у випадку недоступності оригінального немаркованого зображення детектору. Якщо ж вихідне зображення наявне на стороні детектора, то майже завжди можливе порівняння вихідного і заповненого ЦВЗ зображень та інвертування геометричних дій. Однак, частіше стеганографічні методи вимагають можливості виявлення ЦВЗ без доступу до оригінального зображення. Таким чином, зазвичай, не має можливості здійснити зворотні геометричні перетворення, шляхом порівняння вихідного і спотвореного зображень.

Однією із стратегій виявлення ЦВЗ після геометричних спотворень є спроба визначити, які перетворення були застосовані і інвертувати їх перед застосуванням стеганографічного детектора [103]. Це може бути реалізоване за допомогою *вбудовування реєстраційного шаблону* разом із ЦВЗ [104, 105] (рис. 3.7).



а *б* *в*

Рис. 3.7. Вбудовування реєстраційного шаблону (*а* – оригінальне зображення, *б* – зображення, повернуте на 90°, *в* – зображення зі зміною пропорцій)

Проблема лише в тому, що даний метод вимагає вбудовування і виявлення двох ЦВЗ, одного – для реєстрації змін, другого, що несе в собі корисні відомості. Цей підхід може негативно впливати на пропускну здатність та невидимість стеганографічної системи, що слід окремо враховувати. Недоліком цього методу може бути зниження захищеності системи в разі

використання алгоритмом одного й того ж шаблону для всіх зображень-контейнерів. Цей факт може сприяти зловмиснику при наявності в того декількох маркованих зображень. В такому разі він зможе виділити реєстраційний шаблон та видалити його з усіх захищених зображень, знищуючи можливість здійснення зворотних геометричних перетворень [106].

Іншим методом реалізації запропонованої стратегії є *надання ЦВЗ впізнаваної структури* (рис. 3.8). Наприклад, у [107] пропонується вбудовувати ЦВЗ декілька разів у різних просторових областях. Автокореляційна функція заповненого зображення при цьому дасть шаблон піків, що відповідають місцям вбудовування. Зміни в цій моделі піків можуть бути використані для визначення будь-яких афінних спотворень, яким піддавалося марковане зображення. Цей метод має величезний потенціал, але, подібно до описаного вище методу, також має деякі недоліки. Для успішного процесу вилучення прихованого повідомлення необхідно успішне виконання обох процесів, як вилучення ідентифікатора геометричних спотворень, так і самого ЦВЗ після інверсії перетворень [108]. Обидва ці вкладення мають бути міцними і стійкими до підробки. А також в результаті JPEG компресії, якій може піддаватися зображення після вбудовування ЦВЗ, але до процесу детектування, можуть виникнути паразитні піки автокореляції.

а *б* *в* *г* *д*

Рис. 3.8. *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

Очевидно, що методи побудови стеганографічних систем, стійких до геометричних перетворень, а також спотворення значень пікселів зображення, що містить приховане повідомлення, є значною перевагою в реальних додатках.

3.3.2. Аналіз методів підвищення стійкості до завад

Зменшення співвідношення сигнал/шум істотно впливає на якість прийнятого повідомлення. Ступінь відмінності між пустим вхідним контейнером і контейнером з вбудованим секретним файлом збільшується зі зменшенням співвідношення сигнал/шум. Це призводить до збільшення ймовірності помилки у прийнятному повідомленні.

Одним з методів боротьби з цією проблемою є додаткове використання завадостійкого кодування. *Завадостійке кодування* дозволяє за рахунок внесення додаткової надмірності (збільшення мінімальної кодової відстані) у кодових комбінаціях переданих повідомлень забезпечити можливість виявлення та виправлення одиночних, кратних і групових помилок [109].

Для того, щоб при розпакуванні контейнера з отриманої множини символів можна було чітко визначити початок і кінець саме прихованого повідомлення, доцільно вводити визначені секретні мітки, які будуть обмежувати приховану інформацію. Мітки мають складатися з достатньої кількості символів, щоб не було співпадінь з символами прихованої інформації. Крім того, для зменшення ймовірності виявлення міток при проведенні стеганоаналізу бажано, щоб коди цих символів були досить рознесені на ASCII-осі (наприклад, використання поряд з латинськими символами символів кирилиці і службових символів, використання псевдовипадкових послідовностей кодів символів і т. і.).

За рахунок спотворень, внесених шумом в зображення, виникає ймовірність того, що детектор не виявить мітку і не спрацює. Результати

експериментальних досліджень показують, що будь-які дії з об'єктом з дуже великою ймовірністю зачіпають область, в яку були вбудовані мітки початку і кінця корисного повідомлення. А з подальшою зміною її бітової складової, роблять неможливим не тільки декодування, але і виявлення повідомлення. Зміни, що вносяться адитивною завадою також негативно впливають на декодування переданої інформації. Для боротьби з цим можна використовувати *дублювання міток*. При збільшенні кількості міток детектор спрацьовує при меншому співвідношенні сигнал/шум (*Рс/Рш*) [110].

Одним із способів підвищення ймовірності виявлення прихованого повідомлення із спотвореного завадами стеганоконтейнера використовують м’яке детектування. *М’який детектор* показує ймовірність наявності стеганографічного вкладення в сигналі. Принцип м’якого детектування дозволяє виконати правильне детектування та вилучення вкладення навіть за наявності помилок в мітках початку і кінця стеганоповідомлення, оскільки, підвищуючи поріг спрацьовування детектора можна адаптувати його до зашумленості каналу зв'язку [111].

Дослідження методів підвищення завадостійкості систем прихованої інформації було проведене на прикладі метода, що продемонстрував найвищі показники при впливі завад у каналах зв’язку, – методі заміни НЗБ.

На рис. 3.9 показано, як змінюється мінімальне відношення *Рс/Рш*, що потребує детектор, для розпізнавання прихованого повідомлення, в залежності від кількості вбудованих міток.

З підвищенням кількості міток спрацьовування детектора відбувається при менших значеннях співвідношення *Рс/Рш*. У порівнянні з жорстким детектуванням застосування м'якого детектування дозволяє у 1,7 рази зменшити співвідношення *Рс/Рш*, при якому детектор спрацює 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.

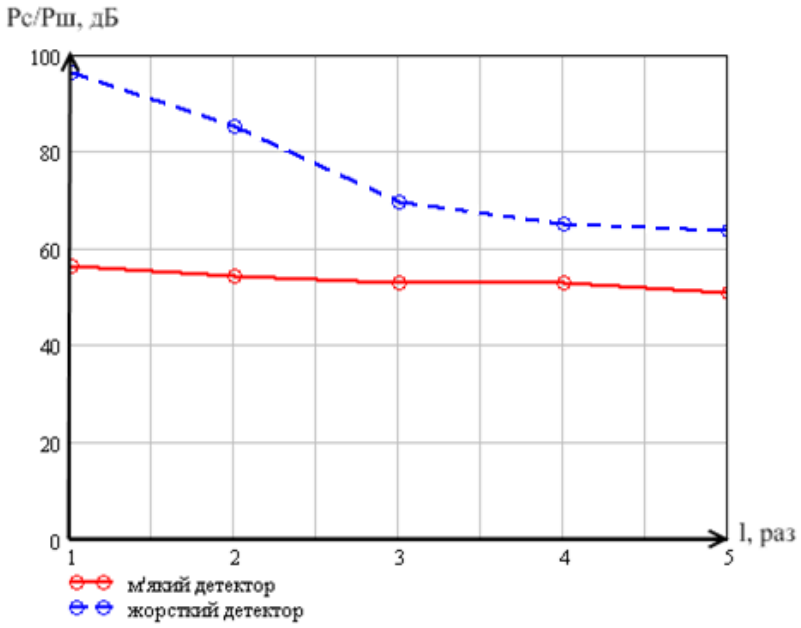


Рис. 3.9. Залежність мінімального значення *Pc/Pш* для спрацьовування м'якого та жорсткого детекторів при дублюванні міток

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).

Експериментальні дослідження показали, що завадостійке кодування дозволяє зменшити ймовірність помилки в прийнятому повідомленні, а також підвищити ймовірність спрацювання детектора при вбудовуванні інформації методом НЗБ (рис. 3.10).

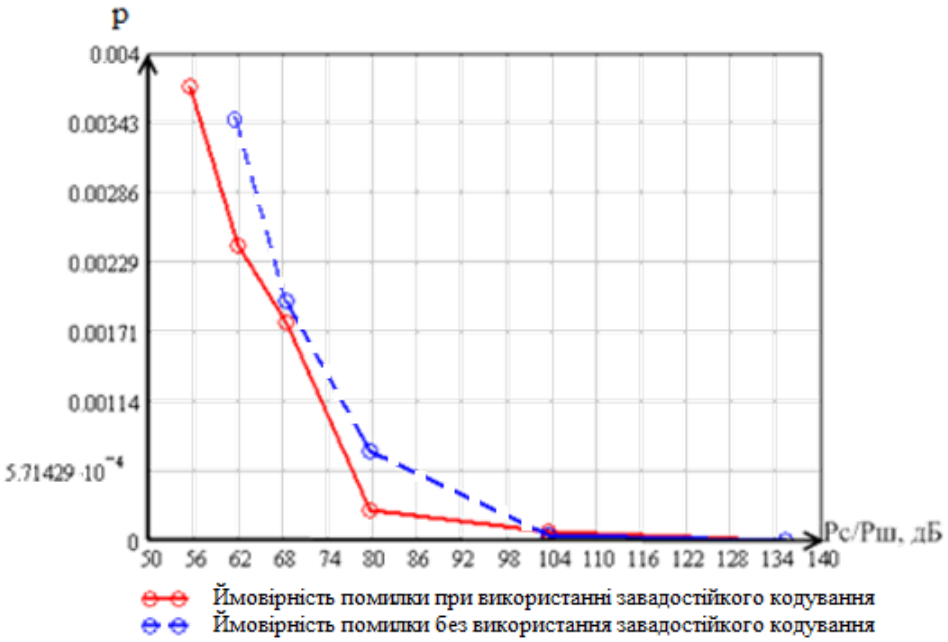


Рис. 3.10. Ймовірності помилки в прийнятому повідомленні при використанні завадостійкого кодування та без нього

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

В контексті аналізу методів підвищення стійкості стеганографічної системи необхідно згадати порогову величину P, яка являє собою різницю між абсолютними значеннями коефіцієнтів ДКП. Ця величина є визначальною при кодуванні біт повідомлення. Вбудовування інформації здійснюється таким чином: для передачі біта «0» прагнуть, щоб різниця абсолютних значень обраних коефіцієнтів ДКП перевищувала величину P, а для передачі біта «1» ця різниця робиться меншою в порівнянні з негативною величиною P:

$$\begin{cases} \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| > P, при\ m_b = 0; \\ \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| < -P, при\ m_b = 1 \end{cases} \quad (3.3)$$

Таким чином, збільшення порогової величини P дозволяє підвищувати стійкість до компресії та впливу завад на можливість детектування та вилучення прихованого повідомлення, проте якість зображення при цьому може значно погіршуватися. Тому необхідно вибирати оптимальну величину P, в залежності від призначення стеганографічної системи.

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

3.3.3. Аналіз методів підвищення пропускної здатності

Для забезпечення додаткової завадостійкості необхідно забезпечити підвищення пропускної здатності, оскільки використання методів завадостійкого кодування чи дублювання інформації вимагає передачі додаткових біт.

В ході досліджень було визначено два методи підвищення пропускної здатності при використанні методів вбудовування в область перетворення.

Перший метод базується на твердженні, що вбудовування у середньочастотні коефіцієнти ДКП забезпечить достатню стійкість зображення, оскільки вони зазвичай не піддаються модифікаціям та втратам збоку алгоритмів стиснення. В той же час людське око не володіє такою високою чутливістю, щоб відчути зміни цих коефіцієнтів. Тому запропоновано метод, що максимально використовує середньочастотні компоненти зображення (рис. 3.11).

	1	2	3	4	5	6	7	8
1	1603	203	11	45	-30	-14	-14	-7
2	108	-93	10	49	27	6	8	2
3	-42	-20	-6	16	17	9	3	2
4	56	69	7	-25	-10	-5	-2	-2
5	-33	-21	17	8	3	-4	-5	-3
6	-16	-14	8	2	-4	-2	1	1
7	0	-5	-6	-1	2	3	0	1
8	9	5	-6	-9	0	3	3	1

- НЧ компоненти;
- СЧ компоненти;
- ВЧ компоненти

Рис. 3.11. Використання 2-х діагоналей СЧ ДКП для вбудовування повідомлення

Другий метод підвищення стійкості зображення використовує для вбудовування не тільки синю матрицю зображення, як це прийнято у загальновідомих методах, але й зелену. Для використання даного методу рекомендується використовувати в якості контейнерів зображення із перевагою зеленого кольору і без великих однотонних ділянок (рис. 3.12).

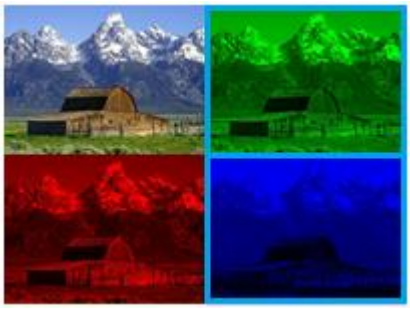


Рис. 3.12. Використання матриці *B* та *G* для вбудовування повідомлення

3.4. Висновки до третього розділу

У третьому розділі дисертаційної роботи були отримані наступні результати:

1. Визначені, класифіковані та досліджені атаки на стеганографічні системи. Отримані кількісні оцінки стійкості до атак проти вбудованого повідомлення та стеганогдетектора, реалізовані на основі афінних перетворень, стисненні та переформатуванні маркованих зображень. За результатами визначено, що при наявності активного порушника, найефективнішим способом приховування даних є методи на основі вейвлет-перетворення.

2. Реалізований програмний комплекс, що імітує канали зв'язку. Що дозволяє дослідити можливість стеганографічних методів адаптуватись до реальних каналів передачі. Були отримані порогові значення спотворень стеганосистем, для яких ще можливе відновлення прихованої інформації. Для різних методів максимально допустиме значення помилки у каналах із стиранням та мультиплікативною завадою становило 0,03-1 %. В той чай, як для каналів із адитивним білим гаусовим шумом помилка не має перевищувати $\sigma_{завади}^2 = 0{,}2$ для всіх досліджуваних методів.

3. Були розраховані мінімальні значення *SNR* для кожного з методів, при якому можливе правильне вилучення прихованої інформації, і максимальні показники *NAD* відповідно.

Загалом найпростіші методи, що оперують із просторовою областю зображення, виявилися найбільш стійкими до обраних завад у комунікаційних каналах. Вони потребують всього 122-126 дБ для значення *SNR*. Метод дискретного вейвлет-перетворення показав значення на рівні найкращих – 286 дБ. В той час, як частотні методи потребують значно вищого рівня *SNR* (264-12431 дБ) для детектування прихованого повідомлення, та мають нижчі граничні показники допустимих спотворень.

4. Набули подальшого розвитку методи підвищення стійкості стеганографічних систем до геометричних атак, де вбудовування реєстраційного шаблону разом із ЦВЗ або надання ЦВЗ впізнаваної структури дозволяють визначити афінні перетворення, які були здійсненні в процесі передачі, і виконати зворотні дії перед застосуванням стеганографічного детектора.

5. 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

6. Вдосконалено 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.

РОЗДІЛ 4
СИНТЕЗ СТЕГАНОГРАФІЧНОГО МЕТОДУ ПЕРЕДАЧІ ДАНИХ, ЕФЕКТИВНОГО ЗА ВИЗНАЧЕНИМИ КРИТЕРІЯМИ

Спираючись на отримані результати у п. 2.3, було вирішено надати подальшого розвитку існуючим методам на основі дискретних перетворень. Методи на основі ДКП та ДВП є досить поширеними [112]. Їх популярність визначається тим, що вони не вносять значних спотворень у зображення, мають достатню пропускну здатність та є стійкими до ряду навмисних атак та викривлень у каналах зв’язку.

У той же час при значному поширенні таких методів в літературі відсутні рекомендації стосовно вибору типу вейвлету та області вбудовування. Також недостатньо розкрите питання порівняльного аналізу методів на основі дискретного косинусного перетворення (ДКП) та дискретного вейвлет-перетворення (ДВП), а також їх комбінованого застосування (ДВП – ДКП).

4.1. Особливості методів вбудовування в область перетворення

Найбільшого поширення серед всіх ортогональних перетворень в стеганографії отримали ДКП і ДВП, що пояснюється значним поширенням їх використання при компресії зображень. Стеганоалгоритм може бути досить стійким до подальшої компресії зображення, тільки якщо він буде враховувати особливості алгоритму перспективного стиснення [89].

В роботі [113] наведено результати численних експериментів, які дозволили авторам дати певні рекомендації щодо вибору виду перетворення для стеганографії (рис. 4.1). Згідно цих досліджень, перетворення можна впорядкувати по досяжним виграшам.

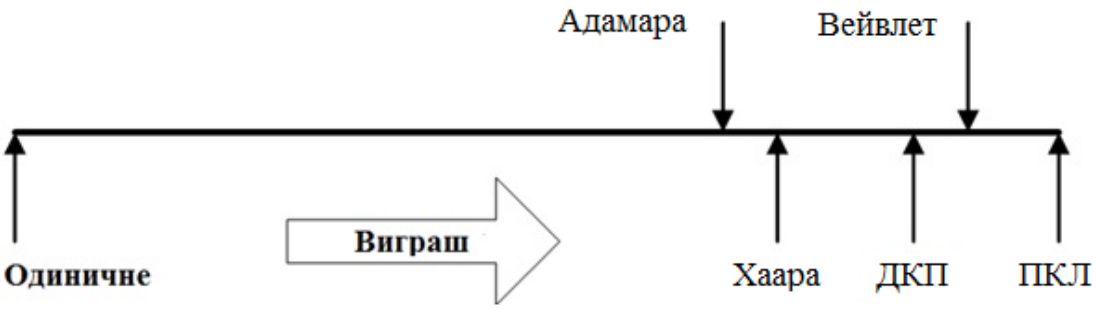


Рис. 4.1. Види перетворень, впорядковані за досяжними виграшам

Перетворення, які характеризуються високими значеннями виграшу, такі як ДКП та ВП характеризуються різко нерівномірним розподілом дисперсій коефіцієнтів піддіапазонів. Високочастотні піддіапазони не підходять для вбудовування через великий шум обробки, а низькочастотні – через високий шум зображення. Тому доводиться обмежуватися середньочастотними діапазонами, у яких шум зображення приблизно дорівнює шуму обробки. Оскільки таких діапазонів небагато, то пропускна здатність стеганоканалу є порівняно малою. У разі застосування перетворення з нижчим виграшем від кодування, наприклад, перетворення Адамара або Фур'є, існує більше блоків, у яких шум зображення приблизно дорівнює шуму обробки, а отже, і пропускна здатність вище.

Ефективність застосування ВП і ДКП для компресії зображень зумовлені тим, що вони добре моделюють процес обробки зображення у зоровій системі людини (ЗСЛ), відділяючи суттєві деталі від другорядних. Таким чином, дані перетворення більш доцільно використовувати в разі присутності активного порушника, оскільки модифікація значущих коефіцієнтів може привести до неприйнятного спотворення зображення.

Найбільш перспективним [89] на даний момент є метод вейвлет-перетворення (ВП).

Вейвлети (від англ. wavelet) – математичні функції, що дозволяють аналізувати різні частотні компоненти даних. Це сімейство функцій, які

локальні в часі і по частоті («маленькі»), і в яких всі функції виходять з однієї, за допомогою її зрушень і розтягувань по осі часу (так що вони «йдуть один за одним»). Іноді вейвлети називають сплесками. Всі вейвлет-перетворення можуть розглядатися як різновид часово-частотного представлення, отже відносяться до предмета гармонійного аналізу [114].

Всі вейвлет-перетворення розглядають функцію (взяту будучи функцією від часу) у термінах коливань, локалізованих за часом і частотою [115].

В основі вейвлет-перетворень, в загальному випадку, лежить використання двох безперервних, взаємозалежних і інтегровних за незалежною змінною функцією [116]:

– вейвлет-функції $\psi(t)$, як *psi*-функції часу з нульовим значенням інтеграла і частотним фур'є-образом $\Psi(\omega)$. Цією функцією, яку зазвичай і називають вейвлетом, виділяються локальні особливості сигналу. В якості вейвлетів зазвичай вибираються функції, добре локалізовані і в часовій, і в частотній області. Приклад часового і частотного образу функції наведено на рис. 4.2.

– масштабуючої функції $\varphi(t)$, як часової скейлинг-функції *phi* з одиничним значенням інтеграла, якою виконується грубе наближення (апроксимація) сигналу.

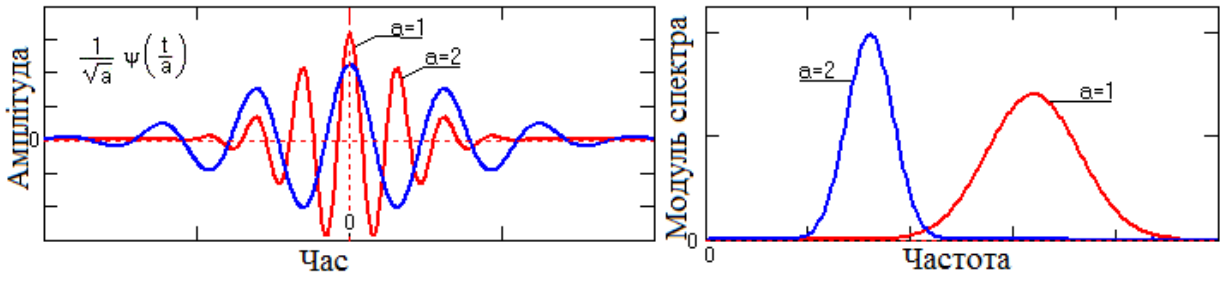


Рис. 4.2. Вейвлетні функції в двох масштабах

Зазвичай виділяють дискретне вейвлет-перетворення (ДВП) і неперервне вейвлет-перетворення (НВП) [117].

Неперервне вейвлет-перетворення (НВП) – реалізація вейвлет-перетворення з використанням довільних масштабів і практично довільних вейвлетів. Вейвлети, що використовуються є неортогональними, а дані, отримані в ході цього перетворення, високо корельованими.

Припустимо, що ми маємо функції $s(t)$ з кінцевою енергією в просторі $L^2(R)$, визначені по всій дійсній осі *R(-∞, ∞)*. Для фінітних сигналів з кінцевою енергією середні значення сигналів повинні наближатися до нуля на ± ∞.

Безперервним вейвлет-перетворенням функції $s(t) \in L^2(R)$ називають функцію двох змінних:

$$C(a,b) = < s(t), \psi(a,b,t) > = \int_{-\infty}^{\infty} s(t)\psi(a,b,t)dt \;\; a,b \in R, a \neq 0, \quad (4.1)$$

де вейвлети $\psi(a,b,t) \equiv \psi_{a,b}(t)$ – масштабовані та зсунуті копії породжуючого вейвлету $\psi(t) \notin L^2(R)$, сукупність яких створює базис простору $L^2(R)$.

Породжуючими функціями можуть бути найрізноманітніші функції з компактним носієм – обмежені за часом і місцем розташування на часовій осі, і мають спектральний образ, локалізований на частотній осі. Базис простору $L^2(R)$ доцільно конструювати з однієї породжуючої функції, норма якої повинна дорівнювати 1. Для перекриття функцією вейвлета всієї часової осі простору використовується операція зсуву (зміщення по часовій осі): $\psi(b,t) \equiv \psi(t-b)$, де значення b для НВП є величиною безперервною. Для перекриття всього частотного діапазону простору $L^2(R)$ використовується операція часового масштабування вейвлета з безперервною зміною незалежної змінної: $\psi(a,t) \equiv |a|^{-1/2} \psi(t/a)$. На рис. 4.1 видно, що якщо часовий образ вейвлета буде розширюватися (зміною значення параметра '*a*'), то його «середня частота» буде знижуватися, а частотний образ (частотна локалізація) переміщуватися на більш низькі частоти. Таким чином, шляхом зсуву по

незалежній змінній $(t-b)$ вейвлет має можливість переміщатися по всій числовій осі довільного сигналу, а шляхом зміни масштабної змінної 'a' (у фіксованій точці $(t-b)$ осі) «переглядати» частотний спектр сигналу за певним інтервалом околиці цієї точки.

З використанням цих операцій вейвлетний базис функціонального простору утворюється шляхом масштабних перетворень і зсувів породжуючого вейвлета $\psi(t)$:

$$\psi(a,b,t) \equiv |a|^{-1/2} \psi[(t-b)/a] \quad a,b \in R, a \neq 0, \psi(t) \in L^2(R). \tag{4.2}$$

Неважко переконатися, що норми вейвлетів $\psi(a,b,t)$ дорівнюють нормі $\psi(t)$, що забезпечує нормувальний множник $|a|^{-1/2}$. При нормуванні до 1 породжуючого вейвлета $\psi(t)$ все сімейство вейвлетів також буде нормованим. Якщо при цьому виконується вимога ортогональності функцій, то функції $\psi(a,b,t)$ утворюють ортонормований базис простору $L^2(R)$ [118].

На рис. 4.3 наведено приклад модельного сигналу і спектра його неперервного вейвлет-перетворення.

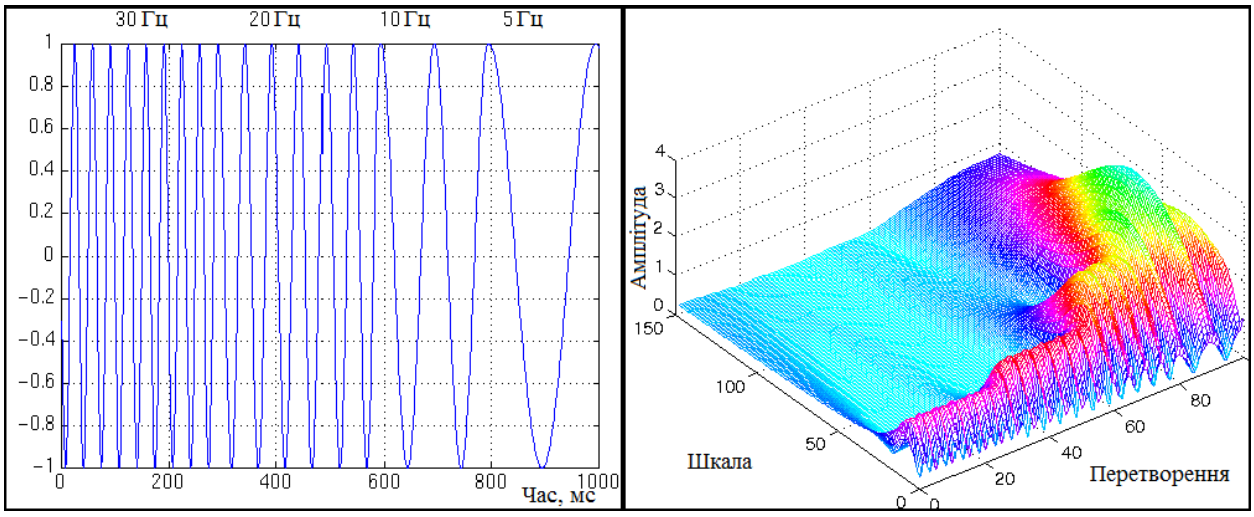


Рис. 4.3. Приклад модельного сигналу і спектра його НВП

Таким чином, неперервне вейвлет-перетворення являє собою розкладання сигналу за всіма можливими зсувами і стисненнями/розтягуваннями деякої локалізованої фінітної функції – вейвлета [119].

Для дискретних часових послідовностей також можна використовувати це перетворення з обмеженням, що найменші переноси вейвлета повинні бути рівні дискретизації даних. Це іноді називається неперервним вейвлет-перетворенням дискретного часу (ДЧ – НВП) і це найчастіше використовуваний метод розрахунку НВП в реальних додатках.

Дискретне вейвлет-перетворення (ДВП). Дискретними прийнято називати вейвлет-перетворення, в яких вейвлети представлені дискретними сигналами (вибірками) [120].

Перше ДВП було придумано угорським математиком Альфредом Хааром. Для вхідного сигналу, представленого масивом 2^n чисел, вейвлет-перетворення Хаара просто групує елементи по 2 і утворює від них суми і різниці. Групування сум проводиться рекурсивно (у разі парної довжини послідовності сум) для утворення наступного рівня розкладання. У підсумку виходить $2^n - 1$ різниця і 1 загальна сума [91].

Найпоширеніший набір ДВП був сформульований бельгійським математиком Інгрід Добеші в 1988 році [92]. Він заснований на використанні рекурентних співвідношень для обчислення все більш точних вибірок неявно заданої функції материнського вейвлета, з подвоєнням дозволу при переході до наступного рівня (масштабу). У своїй основоположній роботі Добеші виводить сімейство вейвлетів, перший з яких є вейвлетом Хаара. З тих пір інтерес до цієї області швидко зріс, що призвело до створення численних нащадків вихідного сімейства вейвлетів Добеші.

ДВП забезпечує достатньо інформації, як для аналізу сигналу, так і для його синтезу, будучи разом з тим економним за числом операцій і необхідної пам'яті. ДВП оперує з дискретними значеннями параметрів a і b, які задаються, як правило, у вигляді степеневих функцій [121]:

$$a = a_0^{-m}, b = k \cdot a_0^{-m}, a_0 > 1, \quad m, k \in I, \tag{4.3}$$

де I – простір цілих чисел {-∞, ∞},

m – параметр масштабу,

k – параметр зсуву.

Базис простору $L^2(R)$ в дискретному поданні:

$$\psi_{mk}(t) \equiv |a|^{m/2} \psi(a_0^m t - k), \quad m, k \in I, \quad \psi(t) \in L^2(R). \tag{4.4}$$

Вейвлет-коефіцієнти прямого перетворення:

$$C_{mk} = \int_{-\infty}^{\infty} s(t) \psi_{mk}(t) dt. \tag{4.5}$$

Значення 'a' може бути довільним, але зазвичай приймається рівним 2, при цьому перетворення називається діадним вейвлет-перетворенням. Для діадного перетворення розроблений швидкий алгоритм обчислень, аналогічний швидкому перетворенню Фур'є, що зумовило його широке використання при аналізі масивів цифрових даних [122].

Зворотне дискретне перетворення для безперервних сигналів при нормованому ортогональному вейвлетному базисі простору:

$$s(t) = \sum_{m=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} C_{mk} \psi_{mk}(t). \tag{4.6}$$

Число використаних вейвлетів за масштабним коефіцієнтом m задає рівень декомпозиції сигналу, при цьому за нульовий рівень (m = 0) зазвичай приймається рівень максимальної часової роздільної здатності сигналу, тобто сам сигнал, а наступні рівні (m < 0) утворюють спадаюче вейвлет-дерево. У програмному забезпеченні обчислень для виключення використання негативної нумерації по m знак «мінус» зазвичай переноситься безпосередньо у (4.7), тобто використовується наступне подання базисних функцій:

$$\psi_{mk}(t) \equiv |a|^{-m/2} \psi(a_0^{-m} t - k), \quad m,k \in I, \quad \psi(t) \in L^2(R). \tag{4.7}$$

Стійкість дискретного базису визначається наступним чином. Функція $\psi(t) \in L^2(R)$ називається *R*-функцією, якщо базис на її основі по (4.4) є базисом Рісса (Riesz). Для базису Рісса існують значення *A* і *B*, $0 < A \le B < \infty$, для яких виконується співвідношення

$$A\|C_{mk}\|^2 \le \left\| \sum_{m=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} C_{mk} \psi_{mk}(t) \right\|^2 \le B\|C_{mk}\|^2, \tag{4.8}$$

якщо енергія ряду C_{mk} кінцева. При цьому для будь-якої *R*-функції існує базис $\psi_{mk}^{\#}(t)$, який є ортогональним базису $\psi_{mk}(t)$. Його називають ортогональним «двійником» базису $\psi_{mk}(t)$, таким, що

$$\left\langle \psi_{mk}(t), \psi_{mk}^{\#}(t) \right\rangle = \delta_{mn} \cdot \delta_{kl} \tag{4.9}$$

Якщо $A = B = 1$ і $a_0 = 2$, то сімейство базисних функцій $\{\psi_{mk}(t)\}$ є ортонормованим базисом і можливе повне відновлення початкового сигналу, при цьому $\psi_{mk}(t) = \psi_{mk}^{\#}(t)$ і для реконструкції сигналів використовується формула (4.6). Якщо $\psi(t)$ не ортогональний вейвлет, але має «двійника», то на базі «двійника» обчислюється сімейство $\psi_{mk}^{\#}(t)$, яке і використовується при зворотному перетворенні замість $\psi_{mk}(t)$, при цьому точне відновлення вихідного сигналу не гарантовано, але воно буде близьке до нього в середньоквадратичному сенсі.

На сьогодні визначені декілька груп методів вбудовування інформації, засновані на різних етапах застосування вейвлет-перетворення. Основні стратегії по застосуванню вейвлетів показані на рис. 4.4 [112].

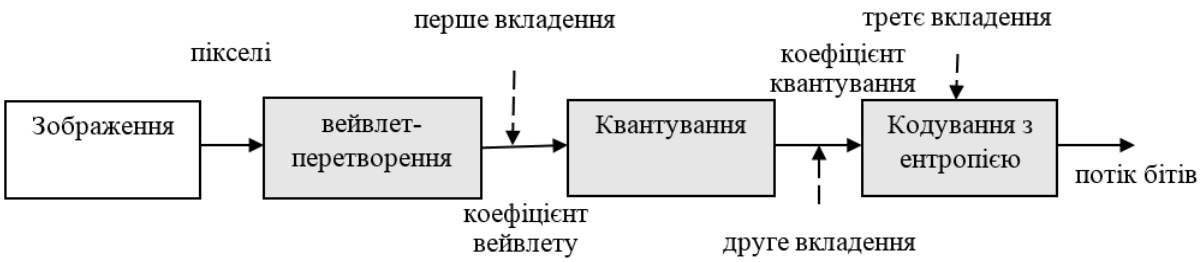


Рис. 4.4. Стратегії вбудовування на основі різних застосувань вейвлет-перетворення для зображень

4.2. Дослідження характеристик методів на основі вейвлет-перетворення

4.2.1. Основні функції вейвлетів

В якості базисних функцій, що утворюють ортогональний базис, можна використовувати широкий набір вейвлетів. Для практичного застосування важливо знати ознаки, якими неодмінно повинна володіти початкова функція, щоб стати вейвлетом. Наведемо основні з них [123].

Обмеженість. Квадрат норми функції повинен бути кінцевим:

$$\|\psi\|^2 = \int_{-\infty}^{\infty} \psi\left|(t)^2\right| dt < \infty. \qquad (4.10)$$

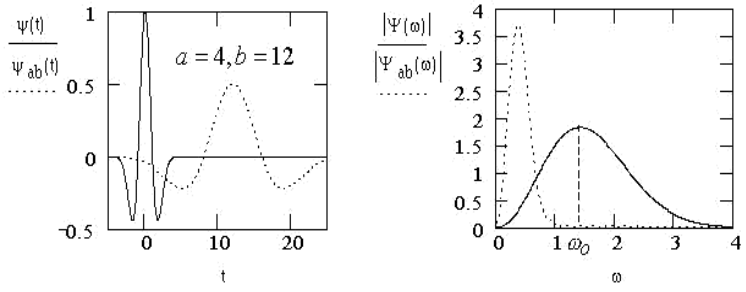
Локалізація. ВП на відміну від перетворення Фур'є використовує локалізовану вихідну функцію і в часі, і за частотою. Для цього достатньо, щоб виконувалися умови:

$$\left|\psi(t)\right| \le C(1+\left|t\right|)^{-1-\varepsilon} \text{ і } \left|S_{\psi}(\omega)\right| \le C(1+\left|\omega\right|)^{-1-\varepsilon}, \text{ при } \varepsilon > 0. \qquad (4.11)$$

Наприклад, дельта-функція $\delta(t)$ і гармонійна функція не задовольняють необхідній умові одночасної локалізації у часовій і частотній областях.

Нульове середнє. Графік вихідної функції повинен осцилювати (бути знакозмінним) навколо нуля на осі часу (рис. 4.5) і мати нульову площу.

$$\int_{-\infty}^{\infty} \psi(t)dt = 0. \qquad (4.12)$$



а *б*

Рис. 4.5. Вейвлет «мексиканський капелюх» (*а*) і модуль його спектральної щільності (*б*)

З цієї умови стає зрозумілим вибір назви «вейвлет» – маленька хвиля.

Рівність нулю площі функції $\psi(t)$, тобто нульового моменту, призводить до того, що Фур'є-перетворення $S_{\psi}(t)$ цієї функції дорівнює нулю при $\omega = 0$ і має вигляд смугового фільтра. При різних значеннях a це буде набір смугових фільтрів.

Часто для додатків буває необхідно, щоб не тільки нульовий, але й всі перші n моментів були рівні нулю

$$\int_{-\infty}^{\infty} t^n \psi(t)dt = 0. \qquad (4.13)$$

Вейвлети n-го порядку дозволяють аналізувати більш тонку (високочастотну) структуру сигналу, пригнічуючи його складові, що змінюються повільно.

Автомодельність. Характерною ознакою ВП є його самоподобність. Всі вейвлети конкретного сімейства $\psi_{ab}(t)$ мають те ж число осциляцій, що і материнський вейвлет $\psi(t)$, оскільки були отримані із нього за допомогою масштабних перетворень (a) і зсуву (b).

Оскільки зображення є набором елементів різного розміру, розташування та орієнтації, то базис вейвлет-перетворення, який передбачає різні масштабні версії, зсуви та форми імпульсів, краще узгоджується з природою такого двомірного сигналу, ніж періодичні функції. Нижче наведено графічне зображення деяких типів вейвлетів (рис. 4.6 та рис. 4.7).

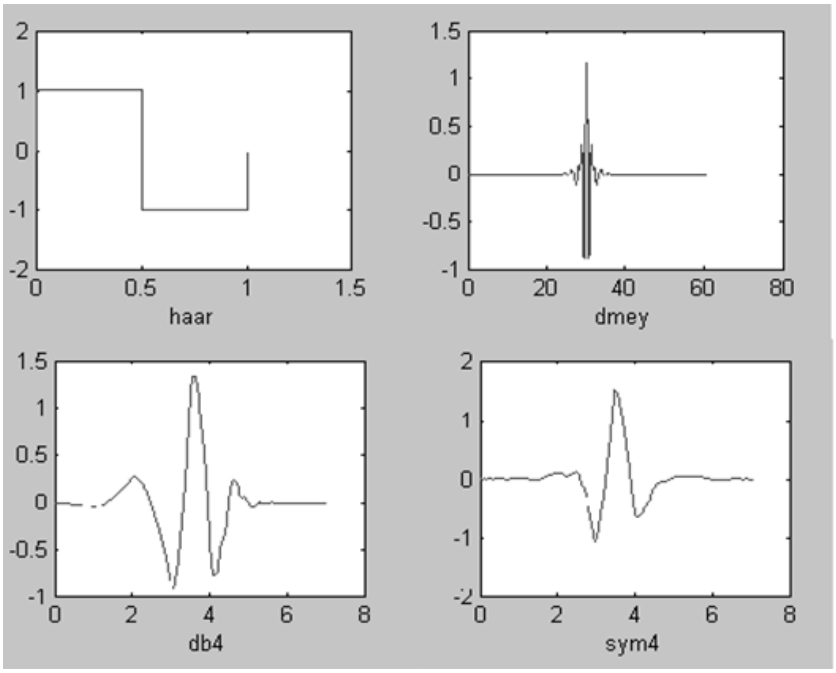


Рис. 4.6. Графічне зображення вейвлетів (де *haar – вейвлет Хаара, dmey – вейвлет Мейєра, db4 – вейвлет Добеші 4-го порядку, sym4 – симлет 4-го порядку)*

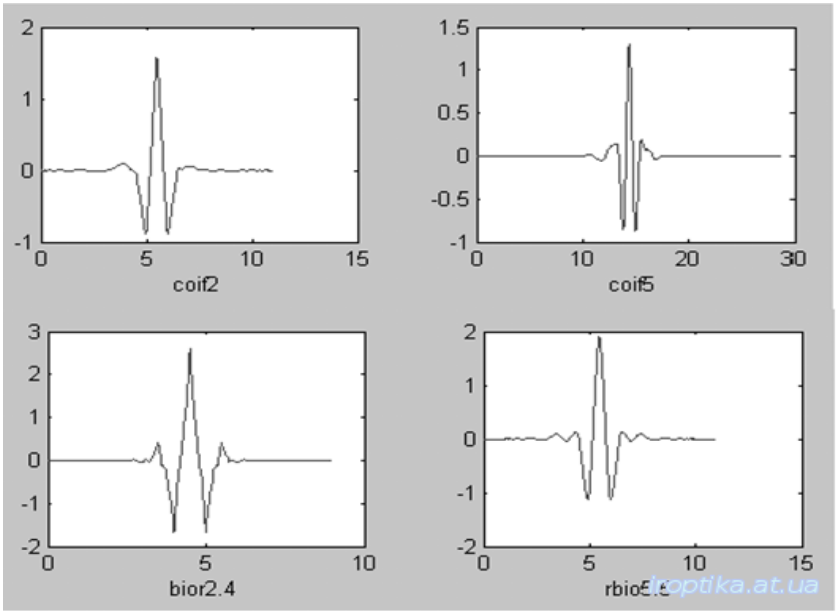


Рис. 4.7. Графічне зображення вейвлетів (де *coif2 та coif5 – коіфлети 2-го та 5-го порядку відповідно, bior2.4 – біортогональний вейвлет, rbio5.6 – обернений біортогональний вейвлет)*

Хоча відомо декілька тисяч різноманітних вейвлетів, на разі кожна система комп'ютерної математики оперує лише з декількома типами вейвлетів [124]. Для досліджень пропонується використовувати чотири родини ортогональних вейвлетів таких типів:

1. Вейвлети Daubechies (Добеші) – родина вейвлетів розроблена Інгрід Добеші. У системі комп'ютерної математики *MathCad* в пакеті *Wavelet Extension* значення змінної, що задає сімейство вейвлетів, дорівнює *daublet(n)*, де *n* – коефіцієнтний вейвлет Добеші (*n* – позитивне парне число від 2 до 20).

2. Вейвлети родини Symlet відомі як асиметричні варіанти вейвлетів Добеші. Значення змінної, що задає сімейство вейвлетів, дорівнює *symmlet(n)*, де *n* – коефіцієнтний вейвлет Добеші з найменшою асиметрією і компактним носієм (*n* – парне число від 4 до 20).

3. Вейвлети родини Coiflet відрізняються від вейвлетів Добеші поліпшеною симетрією. Значення змінної, що задає сімейство вейвлетів, дорівнює *coiflet(n)*, де *n* – коефіцієнтний вейвлет Койфлета (*n* є 6, 12, 18, 24, 30).

4. Вейвлети родини Battle-Lemarie (Бетла-Лємар'є) відомі також як ортогональні сплайнові вейвлети. Змінна *Bspline(n, m)*, що задає сімейство вейвлетів, створює вейвлет *n*-го порядку з 2*m*+1 коефіцієнтами, обидва фільтри якого є лише приблизно ортогональні.

4.2.2. Дослідження характеристик при використанні різних областей вбудовування

При огляді літератури не було знайдено відомостей щодо вибору області вбудовування для стеганографічного вкладення. Отже, актуальним завданням є дослідження зміни параметрів зображення при зміні області вбудовування. Приклад застосування кількаразового вейвлет-перетворення до нерухомого зображення показаний на рис. 4.9.

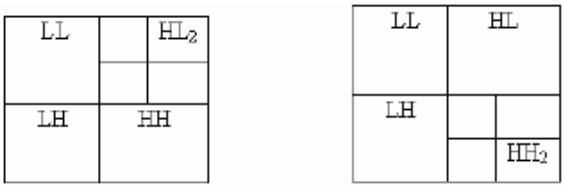
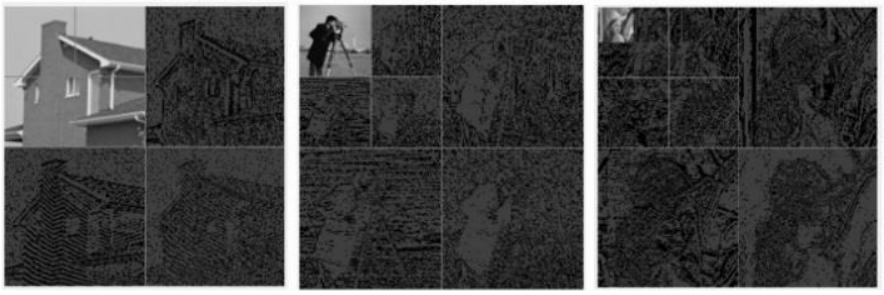


Рис. 4.8. Другий рівень вейвлет-перетворення



а *б* *г*

Рис. 4.9. Результати застосування вейвлетів до зображення
(*а* – 1-го порядку; *б* – 2-го порядку; *в* – 3-го порядку)

Для порівняння були обрані первинні області перетворення LH, HL, HH, та вторинні HL_2 та LH_2 (рис. 4.8). Результат розрахунку нормованої середньої абсолютної різниці *NAD* відображено у вигляді діаграми на рис. 4.10.

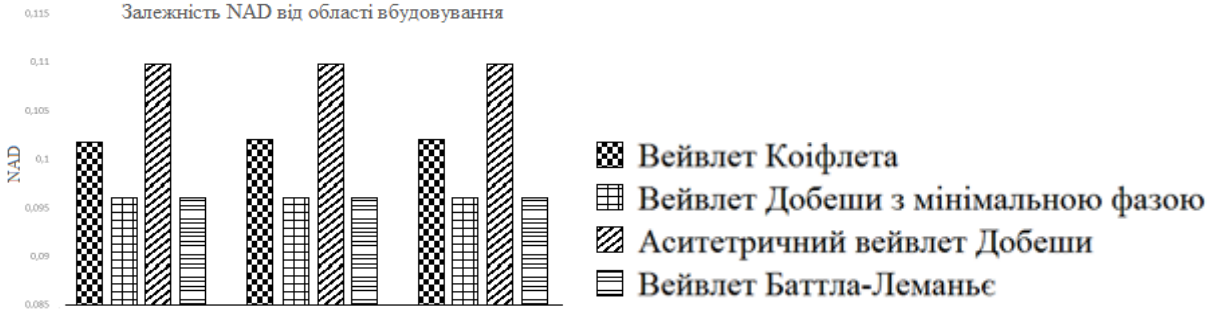


Рис. 4.10. Порівняння параметру NAD при використанні 1-ї (HL_2), 2-ї (LH, HL, HH) та 3-ї області (LH_2)

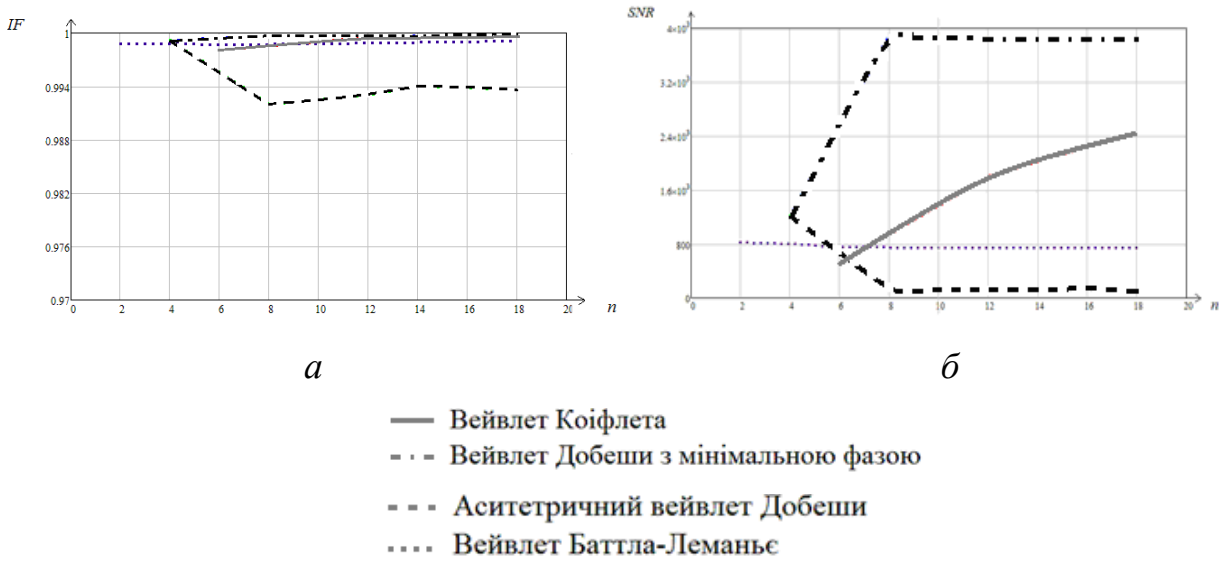
Оскільки величина *NAD* коливається на 0,05% (від 0,095 до 0,1), результатом досліджень можна вважати висновок, що область, в яку вбудовується зображення, не має значного впливу.

4.2.3. Дослідження ефективності використання різних вейвлетів

Вибір конкретного виду і типу вейвлета багато в чому залежить від сигналів, що аналізуються і завдань аналізу, при цьому чималу роль відіграє інтуїція та досвід дослідника. Для отримання оптимальних методів перетворення необхідно визначити певні критерії. В нашому випадку в якості критеріїв вибору вейвлет-функції будемо керуватися значеннями кількісних показників, що були обрані для проведення аналізу стеганографічних методів (п. 1.3).

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) наведені на рис. 4.11.



а *б*

Рис. 4.11. Порівняння параметрів (а – IF, б – SNR) для різних вейвлетів при зміні коефіцієнтів

З графіків залежностей можна нагально виділити вейвлет-функцію Добеши, що дозволяє досягти виграшів параметру *SNR* від 2-х до 5-ти разів. Отже, в подальших реалізаціях методів вбудовування доцільно використовувати саме цю функцію.

4.3. Дослідження характеристик методів вбудовування в область перетворення

Зважаючи на дослідження, проведені у п. 2.3, найкращий результат при комплексному порівнянні методів вбудовування інформації показали методи на основі дискретних перетворень. Для аналізу ефективності методів вбудовування в область перетворення були обрані методи на основі дискретного косинусного перетворення, методи на основі заміни коефіцієнтів вейвлет-перетворення в області середніх коефіцієнтів та послідовного

дискретного вейвлет-перетворення та дискретного косинусного перетворення (ДВП – ДКП) [126].

Метод на основі дискретного косинусного петеворення, що використовувався у дослідженнях, являє собою класичний варіант методу Коха-Жао, і полягає у наступному:

1. Зображення розбивається на блоки розмірністю *8×8* пікселів.

2. До кожного блоку зображення застосовується ДКП, результатом якого є матриці 8×8 коефіцієнтів ДКП.

3. Генеруються дві псевдовипадкові послідовності (ПВП), одна з яких використовується для вбудовування 0, а друга – 1. Кількість елементів у взаємонезалежних ПВП відповідає числу елементів ДКП в блоці.

4. Біти ПВП, збільшені на деякий поріг посилення, складаються зі значеннями обраних коефіцієнтів ДКП.

Наступний метод базується на основі заміни середніх коефіцієнтів вейвлет-перетворення [20] та включає наступні кроки:

1. До зображення застосовується ДВП, результатом якого є розкладання зображення на чотири області.

2. Обрана область (LH/HL/HH) ділиться на блоки *8x8*.

3. Генеруються дві псевдовипадкові послідовності (ПВП), одна з яких використовується для вбудовування 0, а друга – 1. Кількість елементів у взаємонезалежних ПВП відповідає числу елементів ДКП в блоці.

4. Біти ПВП, збільшені на деякий поріг посилення, складаються зі значеннями середніх вейвлет-коефіцієнтів в блоці.

Метод на основі послідовного застосування ДВП – ДКП [5] включає такі кроки:

1. До зображення застосовується ДВП, результатом якого є розкладання зображення на чотири області (рис. 4.12): LL, яка містить зменшене початкове зображення, і три області (LH, HL, HH), які містять результат застосування вейвлету безпосередньо до стовпців, рядків та діагоналі зображення.

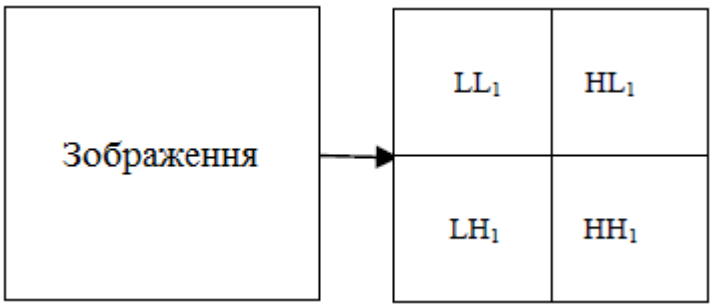


Рис. 4.12. Перший рівень вейвлет-перетворення

2. Обрана область (LH/HL/HH) ділиться на блоки 8x8 і до кожного блоку застосовується ДКП.

3. Генеруються дві псевдовипадкові послідовності (ПВП), одна з яких використовується для вбудовування 0, а друга – 1. Кількість елементів у взаємонезалежних ПВП відповідає числу елементів ДКП в блоці.

4. Біти ПВП, збільшені на деякий поріг посилення, складаються зі значеннями коефіцієнтів ДКП.

4.3.1. Дослідження залежності характеристик від довжини повідомлення

Будь-яка система передачі інформації реалізується із прагненням до максимальної пропускної здатності. Це в свою чергу дозволяє забезпечити високу стійкість до атак, за рахунок можливості багаторазового дублювання цифрового водяного знаку (ЦВЗ).

В Розділі 3 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.

На рис. 4.13 представлені залежності кількісного параметру оцінки якості зображення *SNR* від умовної величини «біт вбудовування на блок зображення».

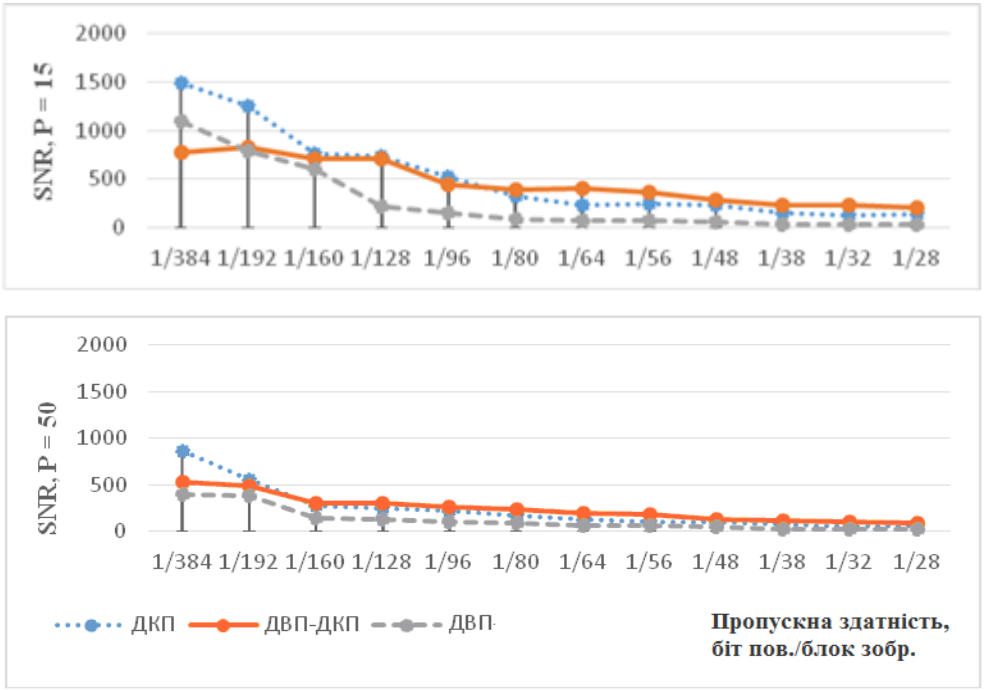


Рис. 4.13. Залежність *SNR* від кількості вбудованих біт на блок зображення

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.

4.3.2. Дослідження залежності характеристик від потужності вбудовування

Як було описано у Розділі 3, ще одним методом підвищення стійкості стеганографічної системи є збільшення порогової величини *P*, яка являє собою різницю між абсолютними значеннями коефіцієнтів ДКП [125].

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. На рис. 4.14 зображені залежності для значення *SNR* від порогу вбудовування при різному об'ємі вкладень.

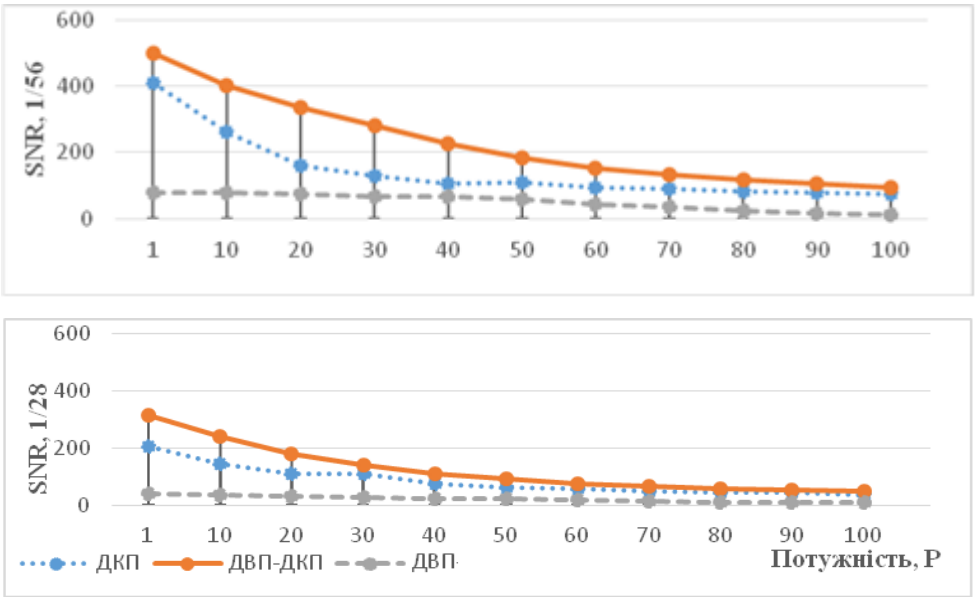


Рис. 4.14. Залежність *SNR* від потужності вбудовування (*а* – при вбудовуванні 1 біта на 56 пікселів зображення, *б* – при вбудовуванні 1 біта на 28 пікселів зображення

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

4.4. Синтез стеганографічного методу, оптимального за сукупністю критеріїв

Спираючись на результати дослідження переваг і недоліків існуючих методів вбудовування інформації був розроблений власний метод стеганографічного приховування інформації. Схема, що відтворює запропонований метод, зображена на рис. 4.15 у вигляді алгоритму. Алгоритм був реалізований у інтегрованому середовищі розробки програмного забезпечення Visual Studio на мові C++. Суть розробленого стеганографічного методу полягає в тому, що зображення та секретна інформація піддаються попередній обробці для підвищення загальної надійності та стійкості стеганосистеми. Синтезований метод утворений шляхом інтеграції запропонованих методів підвищення стійкості, захищеності та пропускної здатності стеганографічних систем.

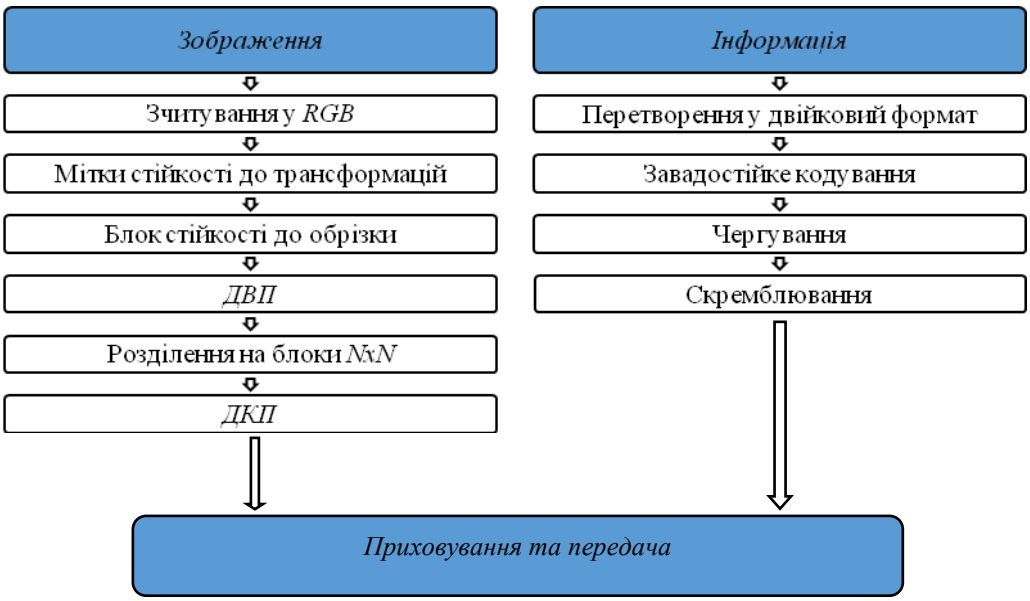
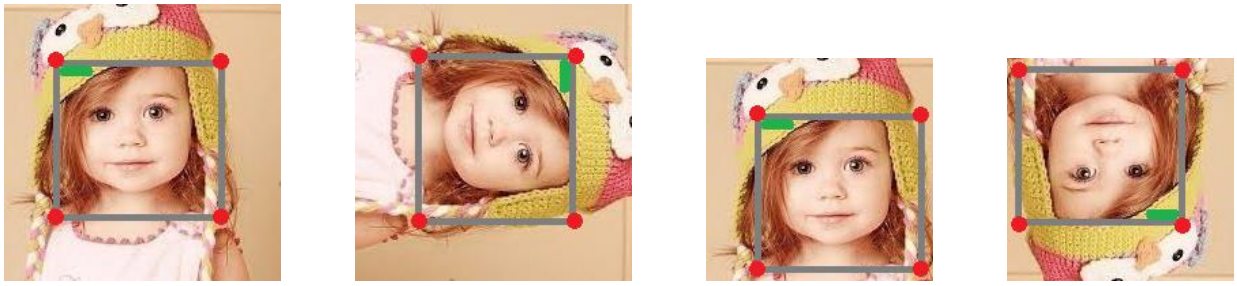


Рис. 4.15. Запропонована стеганографічна система приховування даних у цифрове зображення

Обробка зображення

Зображення зчитується у звичному форматі адитивної колірної моделі *RGB*. В загальному випадку для приховування використовується лише синя компонента зображення *B*.

В ході алгоритму вбудовування передбачається визначення *б*локу стійкості до трансформації. Це дозволяє отримувачу інформації виявити геометричні маніпуляції і виконати зворотні трансформації (якщо можливо), які були виконані із зображенням в процесі передачі. Для цього у зображення впроваджуються мітки у вигляді 4-х точок, що утворюють квадрат, а також мітка, розташована горизонтально з початком у лівому верхньому куті квадрату (рис. 4.16).



а *б* *в* *г*

Рис. 4.16. Впроваджуваний шаблон і приклади трансформацій, які можливо детектувати*: 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°

Одночасно з цим, визначається блок стійкості до обрізки. Він регулюється за допомогою коефіцієнта обрізки *N*, який задається як відсоток пікселів з кожної сторони зображення, які не допустимі для приховування. Цей блок визначає розміри допустимого простору для приховування інформації та обмежується тими самими мітками вершин квадрата.

Таким чином, детектор розпочне роботу тільки після повного відновлення вихідної матриці зображення, шляхом пошуку реєстраційного шаблону – горизонтальної мітки та чотирьох вершин квадрата.

До зображення застосовується дискретне вейвлет-перетворення (ДВП), і обирається область вертикальних (HL_1) і горизонтальних (LH_1) коефіцієнтів перетворення (рис. 4.12).

Безпосередньо вбудовування секретного повідомлення відбувається у коефіцієнти, отримані шляхом застосування ДКП до попередньо підготовленого простору зображення. Для цього, обрані ДВП області зображення-носія (LH_1 та HL_1) розбиваються на блоки розмірами 8×8 пікселів. ДКП застосовується до кожного блоку за формулою (1.10).

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

Далі, на основі секретного ключа генерується псевдовипадкова послідовність, та у відповідності до неї вибирається по одному блоку $\Omega_b(\upsilon,\nu)$ для приховування кожного b-го біту повідомлення.

Під час організації секретного каналу абоненти повинні завчасно домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які використовуватимуться для приховання даних. Дані коефіцієнти задаються їх координатами в масивах коефіцієнтів ДКП: (υ_1,ν_1) і (υ_2,ν_2). Окрім цього, вказані коефіцієнти повинні відповідати косинус-функціям з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЛ областях сигналу, до того ж інформація не спотворюватиметься при *JPEG*-компресії з малими коефіцієнтами стиснення. При реалізації алгоритму змінювалися коефіцієнти $(\upsilon_1=4,\nu_1=5)$ і $(\upsilon_2=5,\nu_2=4)$.

Вбудовування інформації здійснюється таким чином, щоб різниця абсолютних значень коефіцієнтів ДКП перевищувала деяку позитивну

величину P, наприклад P = 50, при передачі біта «0», а для передачі біта «1» ця різниця робиться меншою в порівнянні з цією ж негативною величино P:

$$\begin{cases} \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| > P, при\ m_b = 0; \\ \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2\right| < -P, при\ m_b = 1 \end{cases} \quad (4.14)$$

Обробка інформації

Для підвищення стійкості впроваджуваної інформації до впливу випадкових перешкод в каналі передачі даних, *інформація, що підлягає прихованню,* попередньо кодується кодом корекції помилок. У розробленій системі використовується код Хемінга (8, 12), що дозволяє підвищити ймовірність правильного прийому символу в середньому на 55% із відношенням сигнал/шум в межах 20-40 дБ.

Після застосування завадостійкого коду, ми зменшуємо ймовірність групових помилок і підвищуємо криптографічну стійкість стеганосистеми за допомогою процедур чергування та скремблювання.

4.5. Порівняльний аналіз методів

З метою демонстрації переваг розробленого методу необхідно провести порівняльний аналіз з обраними у Розділі 1 стеганографічними методами вбудовування інформації:

A1 – метод заміни найменш значущих біт (НЗБ) [22, 25];

A2 – метод Куттера-Джордана-Боссена [25, 34];

A3 – метод Коха-Жао [25, 35];

A4 – метод Бенгама-Мемона-Ео-Юнга [25, 36];

A5 – методи із розширенням спектру [40, 41, 42, 93, 94];

A6 – методи, засновані на ДВП [44, 89, 90, 91, 92];

A7 – синтезований метод [5].

4.5.1. Використання багатокритеріальної оптимізації для порівняння стеганографічних методів

На основі інформації, представленої в [24, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 80, 81, 82, 83], та використовуючи метод присвоєння коефіцієнтів факторам, була створена табл. 4.1. Значення коефіцієнтів були отримані способом, аналогічним описаному у п. 2.3.

Таблиця 4.1

Порівняльний аналіз методів вбудовування

	a	*b*	*c*	*d*	*e*	*f*
A1	8	1	6	1	8	8
A2	7	4	6	4	7	7
A3	2	6	4	6	5	5
A4	1	5	5	6	4	4
A5	6	6	7	5	3	3
A6	6	7	7	8	2	2
A7	1	8	8	8	1	1

Де: *a* – пропускна здатність; *b* – стійкість; *c* – невидимість; *d* – захищеність; *e* – складність вбудовування; *f* – складність виявлення.

У табл. 4.2 показник «8» є найкращим значенням характеристики, «1» – найгіршим.

Багатокритеріальний порівняльний аналіз обраних методів *A1* – *A7* проводився на основі даних, наведених у табл. 4.1. Для цього використовувалася методика попарних порівнянь, описана у п. 2.2.2. На початковому етапі порівняльний аналіз обраних методів виконувався окремо для кожної стеганографічної характеристики. Приклад оцінки стійкості та захищеності показано у вигляді матриць в табл. 4.2 та табл. 4.3 відповідно.

Таблиця 4.2

Матриця порівняння методів (за стійкістю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		1/4	1/6	1/5	1/6	1/7	1/8
A2	4		1/3	1/2	1/3	1/4	1/5
A3	6	3		2	1	1/2	1/3
A4	5	2	1/2		1/2	1/3	1/4
A5	6	3	1	2		1/2	1/3
A6	7	4	2	3	2		1/2
A7	8	5	3	4	3	2	

Таблиця 4.3

Матриця порівняння методів (за захищеністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		1/4	1/6	1/6	1/5	1/8	1/8
A2	4		1/3	1/3	1/2	1/5	1/5
A3	6	3		1	2	1/3	1/3
A4	6	3	1		2	1/3	1/3
A5	5	2	1/2	1/2		1/4	1/4
A6	8	5	3	3	4		1
A7	8	5	3	3	4	1	

Матриці попарних порівнянь, отримані для інших характеристик наведені в Додатку Д.

Результуючі оцінки методів *A1 – A7* за окремими характеристиками були отримані за формулою (2.14). Підсумовуючи значення всіх параметрів (2.23) та виконуючи їх нормування, отримали параметри оцінки якості методів, що наведені в табл. 4.4. Найбільші значення в табл. 4.4 є найліпшими.

Таблиця 4.4

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)*, 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.

4.5.2. Кількісні оцінки

Для порівняльного оцінювання якості стеганографічних засобів можна використовувати загальновідомі показники, що дають кількісні оцінки [25]. Вони оперують із зображеннями на рівні пікселів. Формули та визначення параметрів наведені у п. 1.3.1.

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*.

Отже, отримані результати запропонованих характеристик наведені в табл. 4.5 (тестове зображення розміром *128x128*, контейнер заповнений повністю).

Таблиця 4.5

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. 4.5

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, отримані шляхом побітового порівняння оригінального та спотвореного контейнеру, можна зробити висновок, що розроблений метод є стійким до статистичного аналізу і не видає прихованого повідомлення суттєвими відхиленнями показників.

4.5.3. Порівняння завадостійкості стеганографічних систем передачі

Аналогічно дослідженням, проведеним у п. 3.2 необхідно оцінити можливість розробленого методу адаптуватись до реальних каналів зв'язку та порівняти отримані значення з показниками, що демонструють існуючі методи. Для цього використовувався програмний засіб, що імітує канали, описані у п. 3.2.

Порогові значення спотворень, для яких ще можливе відновлення прихованої інформації, наведені в табл. 4.6.

Таблиця 4.6

Порогові значення спотворень контейнера для відновлення інформації

Метод	Канал з АБГШ, $\sigma_{завади}^2$	Канал із мультиплікативною завадою, $P_{помилки}$, %	Канал із стираннями, $P_{стирання}$, %
A1	0,2	1	1
A2	0,2	1	1
A3	0,2	0,3	0,3
A4	0,2	0,03	0,03
A6	0,2	0,5	0,5
A7 (P=50)	0.2	1,4	1,4

Аналогічно попередньо проведеним дослідженням були розраховані кількісні показники для оцінки методів. На рис. 4.17 та рис. 4.18 представлені графіки усереднених характеристик *SNR* та *NAD* на порогових значеннях спотворень контейнерів. Тобто по осі ординат відкладені мінімальні значення *SNR* для кожного з методів, при якому можливе правильне вилучення прихованої інформації (рис. 4.17), і максимальні показники *NAD* відповідно (рис. 4.18).

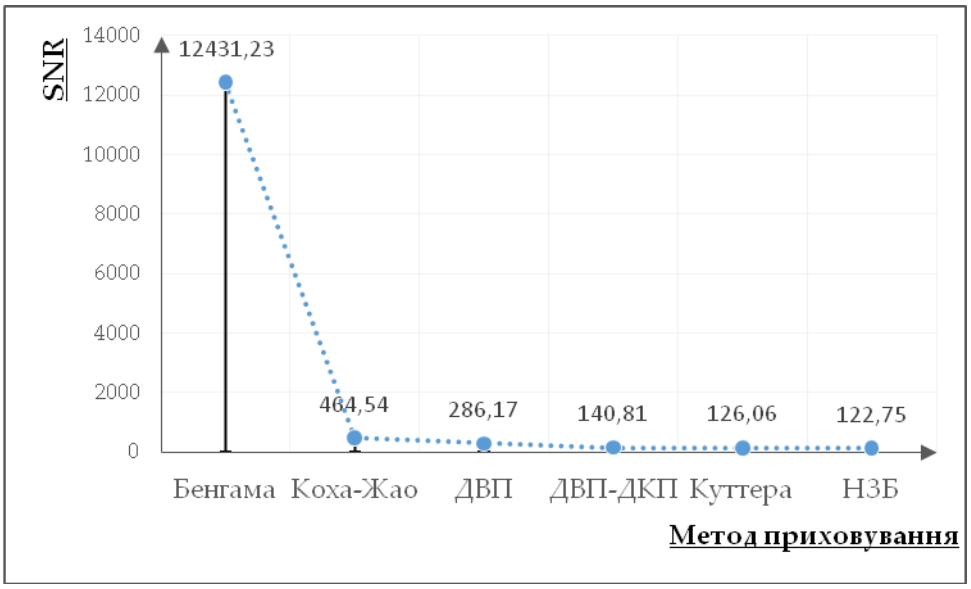


Рис. 4.17. *SNR* для порогових значень спотворень для кожного з методів

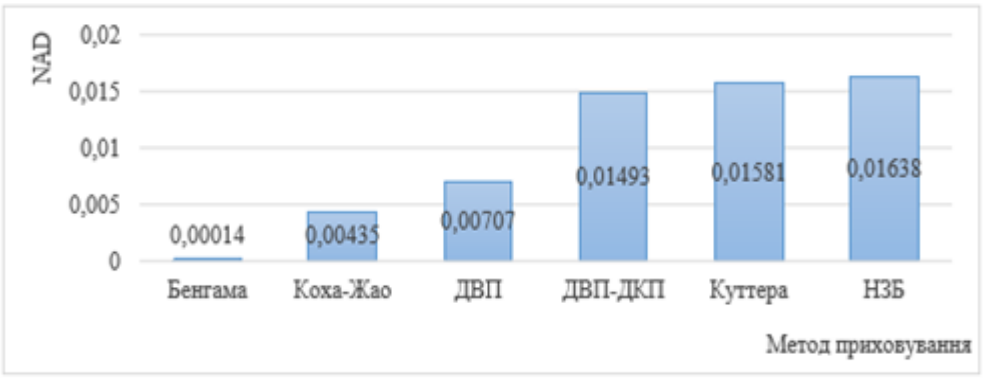


Рис. 4.18. *NAD* для порогових значень спотворень для кожного з методів

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.

Також значним досягненням є впровадження можливості детектувати і успішно здійснювати вилучення прихованого повідомлення, навіть при поворотах і обрізці зображення (табл. 4.7), що раніше унеможливлювало сам процес виявлення наявності прихованих вкладень.

Таблиця 4.7

Стійкість до атак

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

4.6. Висновки до четвертого розділу

У четвертому розділі дисертаційної роботи були отримані наступні результати:

1. Вперше отримано кількісні оцінки впливу вибору області вбудовування на невидимість стеганографічних вкладень. Для порівняння були обрані первинні LH, HL, HH, та вторинні HL_2 та LH_2 області перетворення. Результатом досліджень можна вважати, що область, в яку вбудовується зображення, не має значного впливу на якість заповненого зображення.

2. Отримані кількісні залежності параметрів стеганографічних систем на основі ДВП від використання різних вейвлет-функцій (вейвлета Коіфлета, Батла-Лємар'є, асиметричного вейвлета Добеші та вейвлета Добеші із мінімальною фазою). Було виділено вейвлет-функцію Добеши, що дозволяє досягти виграшів параметру *SNR* від 2-х до 5-ти разів.

3. Розраховані залежності кількісного параметру оцінки якості зображення *SNR* від умовної величини «біт вбудовування на блок зображення» для 3-х методів ДКП, ДВП та їх послідовного застосування. З отриманих залежностей випливає, 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.

4. Визначено, що метод на основі комбінованого використання ДВП та ДКП, дозволяє максимально збільшити порогову величину *P* без істотних візуальних спотворень зображення. Дослідження проводилися на основі розрахунку залежності *SNR* від потужності вбудовування.

5. Вдосконалено метод підвищення стійкості стеганографічних систем до геометричних атак, що відрізняється вбудовуванням реєстраційного шаблону разом із цифровим водяним знаком, також 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 передбачає 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.

7. Для об’єктивного підтвердження переваг запропонованого методу були розраховані кількісні та якісні показники існуючих та запропонованої стеганографічної системи. На основі чого був проведений порівняльний аналіз. Синтезований метод показав відмінні результати відносно найпоширеніших методів та проявив стійкість до статистичного стеганоаналізу, не виявивши суттєвих відхилень розрахованих показників.

На підставі отриманих результатів багатокритеріальної оцінки можна впевнено стверджувати, що метод, заснований на послідовному застосуванні ДВП та ДКП (*A7*) показав найкращі властивості за стійкістю (R = 0,416), невидимістю (R = 0,376) та захищеністю (R = 0,345) стеганографічної системи відносно інших найпоширеніших методів приховування інформації для передачі в мережі зв'язку.

8. Була оцінена можливість розробленого методу адаптуватись до реальних каналів зв’язку та виконане порівняння отриманих значення з показниками, що демонструють існуючі методи.

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.

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

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 ВИКОРИСТАНИХ ДЖЕРЕЛ

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.

22. Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.

23. Fidrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fidrich. – Cambridge: Cambride University Press, 2009. – 438 p.

24. Fridrich J. Applications of Data Hiding in Digital Images / J. Fridrich // Tutorial for the ISPAC S'98 Conferece. – Melbourne, Australia, 1999. – 33 p.

25. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.

26. Kuhn M.G., Stirmark", available at http://www.cl.cam.ac.uk/~mgk25/stirmark/. – Security Group, ComputerLab, Cambridge University, UK (E -mail: mkuhn@acm.org), 1997.

27. Craver S. Can Invisible Watermarks Resolve Rightful Ownerships? / S. Craver, N. Memon, B. Yeo, M. Yeung // International Society for Optics and Photonics. – Electronic Imaging'97, 1997. – P. 310 – 321.

28. Fridrich J. Robust digital watermarking based on key-dependent basis functions / J. Fridrich // The 2nd Information Hiding Workshop. – Portland, Oregon, April 15 – 17, 1998. – P. 168 – 190.

29. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М: Радио и связь, 2003. – 152 с.

30. Osborne C. A Digital Watermark / C. Osborne, R. van Schyndel, A. Tirkel // IEEE International Conference on Image Processing. – Austin, Texas, 1994. – vol.3. – P. 86 – 90.

31. Зайцева Е.А. Компьютерная графика: учеб.-метод. пособие / Е.А. Зайцева, Т.Г. Пунина. – Тамбов: ТГТУ, Пед. Интернет-клуб, 2006. − 116 с.

32. Основи комп'ютерної графіки: навч. посіб. / В.С. Березовський, В.О. Потієнко, І.О. Завадський; за заг. ред. А.М. Гуржія. − К.: BHV, 2009. − 400 с.

33. Jadav Y. Comparison of LSB and Subband DCT Technique for Image Watermarking / Y. Jadav // Conference on Advances in Communication and Control Systems 2013. − 2013. − P. 398 − 401.

34. Kutter M. A fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents. − San Jose, France, 1999. – vol. 3657 − P. 226 – 239.

35. Koch E. Toward robust and hidden image copyright labeling / E. Koch, J. Zhao // Proc. of IEEE Workshop on Nonlinear Signal and Image Processing. − Neos Marmaras, Greece, 1995. − P. 456 − 459.

36. Benham D. Fast watermarking of DCT-based compressed images / D. Benham, N. Memon, B. L. Yeo, M. Yeung // Proc. of Int Conf Image Science, Systems, and Technology. − Las Vegas, NV, 1997. − P. 243 − 253.

37. . Sridevi T. A Robust Watermarking Algorithm Based on Image Normalization and DC Coefficients / T. Sridevi, V. Kumar // IJCSI International Journal of Computer Science. – 2011. – vol. 8, Issue 5, No 2. – P. 226 – 232.

38. Li Z. A Dynamic Multiple Watermarking Algorithm Based on DWT and HVS / Z. Li, Y. Xilan, L. Hongsong, C. Minrong // Int. J. Communications, Network and System Sciences. – 2012. – 5. – P. 490 – 495.

39. Kashyap N. Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT) / N. Kashyap, G.R. Sinha // I.J. Modern Education and Computer Science. – April, 2012. – vol.3. – P. 50 – 56.

40. . Fridrich J. Comparing robustness of watermarking techniques / J. Fridrich, M. Goljan // Proc. SPIE (Security and Watermarking of Multimedia Content). – San Jose, 1999. – vol. 3657. – P. 214 – 225.

41. Ó Ruanaidh J. Rotation, scale and translation invariant digital image watermarking / J. Ó Ruanaidh, T. Pun // Proc. of the ICIP'97. – California, 1997. – vol. 1, P. 536–539.

42. Piva A. Threshold Selection for Correlation-Based Watermark Detection / A. Piva, M. Barni, F. Bartolini // Proceedings of COST 254 Workshop on Intelligent Communications. – L'Aquila, Italy, 1998. – P. 67 – 72.

43. Watermarking (Vol.1) / Edited by Das Gupta, M. – Croatia: InTech, 2012. – 212 p.

44. Лагун А. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А. Лагун, І. Лагун // Захист інформації і безпека інформаційних систем. – Л., 2013. – С. 98 – 99.

45. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, О.Г. Корченко, В.В. Волянська // Захист інформації. – 2012. – №1. – С. 108 – 121.

46. Кини Р.Л. Принятие решений при многих критериях предпочтения и замещения / Р.Л. Кини, Х. Райфа – М.: Радио и связь, 1981. – 560 с.

47. Тоценко В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / В. Г. Тоценко. – Киев: Наук. думка, 2002. – 381 с.

48. Гафт М.Г. Принятие решений при многих критериях / М.Г. Гафт. – М.: Знание, 1979. – 64 с.

49. Тухвалов М.Б. Весовые методы в математическом программировании / М.Б. Тухвалов. – Ташкент: ФАИ, 1981. – 158 с.

50. Zeleny M. Compromise programming in M.K. Starr and M. Zeleny, Eds., Multiple Decision Making / M. Zeleny. – Columbia: University of South Carolina Press, 1973. – 816 p.

51. Литвак Б.Г. Экспертная информация. Методы получения и анализа / Б.Г. Литвак. – М.: Радио и связь, 1982. – 185 с.

52. Методы определения коэффициентов важности критериев / А.М. Анохин, В.А. Глотов, В.В. Павельев [и др.] // Журнал Автоматика и телемеханика. – Москва, 1997. – № 8. – С. 3 – 35.

53. Урицкая О.Ю. Теория принятия решений: учеб.пособие / О.Ю. Урицкая. – СПб.: СПбГТУ, 1999. – 93 с.

54. Мандель И.Д. Кластерный анализ / И.Д. Мандель. – М.: Финансы и статистика, 1988. – 176 с.

55. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ООО "ТИД "ДС",

2002 – 688 с.

56. Wei T.H. The algebraic foundations of ranking theory: thesis (Ph.D.) / T.H. Wei. – Cambridge, 1952.

57. Saaty T.L. Eigenvector and logarithmic least squares / T.L. Saaty // Eur. J. Oper. Res. 1990. – vol. № 1. – P. 156 – 160.

58. Cogger K.O. Eigenweight vectors and least-distance approximation for revealed preference in pairwise weight rations / K.O. Cogger, P.L. Yu // J. Optimiz. Theory and Appl. – 1985. – vol.46. – №4. – P. 483 – 491.

59. Юшманов С.В. Метод нахождения весов, не требующий полной матрицы попарных сравнений / С.В. Юшманов // Автоматика и телемеханика. – М.: Наука, 1990. – №2. – С. 186 – 189.

60. Берж К. Теория графов и ее применения / К. Берж. – М.: Изд-во иностр. лит., 1962. – 320 с.

61. Churchmen C.W. An approximate Measure of Value / C.W. Churchmen, R. Ackoff // Operations Research. – 1954. – №2. – P. 171 – 181.

62. Nelson W.L. On the use of optimization Theory for Practical Control System Design / W.L. Nelson // IEEE, Trans. on Automatic Control. – 1964. – vol. AC-9. – № 4. – P. 469 – 477.

63. Подиновский В.В. Лексикографические задачи линейного программирования / В.В. Подиновський // журн. вычисл. матем. и мат. физики. – 1972. – Т.12, №6. – С. 568 – 571.

64. Орлов А. И. Теория принятия решений: учебник / А. И. Орлов. – М.: Экзамен, 2006. – 573 с.

65. Юттлер Х. Линейная модель с несколькими целевыми функциями / Х. Юттлер // Экономика и мат. методы. – 1977. – Т.3, №3. – С. 356 – 361.

66. Сербин И.В. Оценка значимости факторов в маркетинговых исследованиях банков / И.В. Сербин // Сб. науч. труд. – Пятигорск: СевКавГТУ. – 2005. – № 2. – С. 54 – 60.

67. Гермеер Ю.Б. Введение в теорию исследования операций / Ю.Б. Гермеер. – М.: Наука, 1971. – 324 с.

68. Charsnes A. Management models and industrial applications of line programming / A. Charsnes, W.W. Cooper. – N.Y.: Wiley, 1961. – P. 35 – 41.

69. Szidarovszky F.I. Use of cooperative games in a multiobjective analysis of maning and environment / F.I. Szidarovszky, Bogardi, L. Duckstein // Proc. and International Conference on Applied numerical Modeling. Madrid. Spain. – 1978. – № 9. – P. 11 – 15.

70. Thurstone L.L. The measurement of valnes / L.L. Thurstone. – Chicago: The University of Chicago Press, 1959. – 322 p.

71. Глотов В.А. Метод определения коэффициентов относительной важности / В.А. Глотов // Приборы и системы управления. – 1976. – №8. – С. 17 – 22.

72. Rosner B.S. A new scaling technique for absolute judgement / B.S. Rosner // Psychometrica. – 1956. – vol. 21, №4. – P. 377 – 381.

73. Тутыгин А.Г. Преимущества и недостатки метода анализа иерархий / А.Г. Тутыгин, В.Б. Коробов // Известия Российского государственного педагогического университета им. А.И. Герцена. – Санкт-Петербург, 2010. – Вып. 122. – С. 108 – 115.

74. Саати Т. Аналитическое планирование / Т. Саати, К. Кернс. – М.: Радио и связь, 1991. – 224 с.

75. Базара М. Нелинейное программирование. Теория и алгоритмы / М. Базара, К. Шетти. – М.: Мир, 1982. – 583 с.

76. Голуб Дж. Матричные вычисления / Дж. Голуб, Ч. Ван Лоун. – М.: Мир, 1999. – 548 с.

77. Тихомирова А.Н. Стратегия принятия решений в условиях неопределенности: дис. канд. экон. наук; спец. 08.00.13. – Математические и инструментальные методы экономики / А.Н. Тихомирова, Е.В. Сидоренко // Интеллектуальные технологии в образовании, экономике и управлении. – 2009. – С. 363 – 366.

78. Donegan H.A. A note on Saaty’s random indexes / H.A. Donegan, F.J. Dodd // Mathl. Comput. Modelling. – 1991. – vol. 15, No 10. – P. 135 – 137.

79. Коробов В.Б. Сравнительный анализ методов определения весовых коэффициентов. «влияющих факторов» / В.Б. Коробов // Социология. – 2005. – № 20. – С. 54 – 72.

80. Сейеди С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – БГУИР, 2013. – С. 66 – 75.

81. Singh P. Survey of Digital Watermarking Techniques, Applications and Attacks / /P. Singh, R.S. Chadha // International Journal of Engineering and Innovative Technology (IJEIT). – 2013. – vol. 2, Issue 9. – P. 165 – 175.

82. Kanzariya Nitin K. Comparison of Various Images Steganography Techniques / K. Kanzariya Nitin, V. Nimavat Ashish // International Journal of Computer Science and Management Research. – 2013. – vol. 2, Issue 1. – P. 1213 – 1217.

83. Stuti G. A Review of Comparison Techniques of Image Steganography / G. Stuti, R. Arun, K. Manpreet // IOSR Journal of Electrical and Electronics Engineering. –2013. – vol. 6, Issue 1. – P. 41 – 48.

84. Химмельблау Д. Анализ процессов статистическими методами / Д. Химмельблау. – М.: мир, 1973. – 468 с.

85. Digital Watermarking and Steganography. Second Edition / I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker. – Elsevier, 2008. – 592 p.

86. Singh P. Survey of Digital Watermarking Techniques, Applications and Attacks / P. Singh, R.S. Chadha // International Journal of Engineering and Innovative Technology (IJEIT). – 2013. – vol. 2, Issue 9. – P. 165 – 175.

87. Dittmann J. Media-independent Watermarking Classification and the need for combining digital video and audio watermarking for media authentication / J. Dittmann, A. Mukherjee, M. Steinebach // German National Research Center for Information Technology. – Las Vegas, NV 2000. – P. 62 – 67.

88. Image Steganography Techniques: An Overview / H. Nagham, Y. Abid, R. Badlishah Ahmad, Osamah M. Al-Qershi // International Journal of Computer Science and Security. – 2012. – vol. 6, Issue 3. – P. 168 – 187.

89. Добеши И. Десять лекций по вейвлетам / И. Добеши. – Ижевск, 2011. – 464 с.

90. Лукічов В.В. Методи та засоби стеганографічного захисту інформації в комп'ютерних системах і мережах на основі вейвлет-перетворень / В.В. Лукічов // автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21. – К., 2010. – 20 с.

91. Тхи Тху Чанг Буй Разложение цифровых изображений с помощью думерного вейвлет-преобразования и быстрого преобразования Хаара / Тхи Тху Чанг Буй, В.Г. Спицын // Томский политехнический институт. – 2011. – №5, т.318. – С. 73 – 76.

92. Daubechies I. Orthonormal basis of compactly supported wavelets / I. Daubechies // Comm. Pure Appl. Math, v. XLI. – 1988. – P. 909 – 996.

93. Fridrich J. Secure steganographic methods for palette images / J. Fridrich, D. Rui // In Inter'l Workshop on Information Hiding. – 1999. – P. 47 – 60.

94. Marvel L.M. / Capacity of the additive steganographic channel, Methodology of Spread-Spectrum. Image Steganography / L.M. Marvel, C.G. Boncelet, Jr. Charles, T. Retter // Proc. of IEEE transactions on image processing, August 1999. – 1999. – *v*ol.8, No.8. – P. 1075 – 1083.

95. Завади [Електронний ресурс] // Вікіпедія. – 2013. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Завади.

96. Стеганография [Електронний ресурс] // Вікіпедія. – 2016. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Стеганография.

97. Surekha B. A Spatial Domain Public Image Watermarking / B. Surekha, G.N. Swamy // International Journal of Security and Its Applications. – 2011. – vol. 5 No. 1. – P. 1 – 12.

98. Ching-Yung L. Rotation, Scale, and translation resilient public watermarking for images / L. Ching-Yung, Min Wu, J.A. Bloom and other // IEEE Transactions on image processing. – 2000. – vol.10, No.5. – P. 767 – 782.

99. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / А. А. Гладких. – Ульяновск : УлГТУ, 2010. – 379 с.

100. Теория электрической связи: учебное пособие / К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко;под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ,1 2008. – 452 с.

101. Ching-Yung L. Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection / L. Ching-Yung. – Columbia University. – 2000. – 258 p.

102. Ching-Yung L. Rotation, Scale, and translation resilient public watermarking for images / L. Ching-Yung, Min Wu, J.A. Bloom and other // IEEE Transactions on image processing. – 2000. – vol.10, No.5. – P. 767 – 782.

103. Kutter M. Watermarking resisting to translation, rotation, and scaling / M. Kutter // Signal Processing Laboratory. – Switzerland, 1998. – 10 p.

104. Pereira S., Pun T., Fast Robust Template Matching for Affine Resistant Image Watermarks / S. Pereira, T. Pun // Proc. Of the 3th Int. Information Hiding Workshop. – 1999. – P. 207 – 218.

105. A Bayesian Approach to Affine transformation Resistant Image and VideoWatermarking / G. Csurka, F. Deguillaurne, J.J.K. O'Ruanaidh, T. Pun // Proc. Of the 3th Int. Information Hiding Workshop. – 1999. – P. 315 – 330.

106. Fridrich J. Methods for Detecting Changes in Digital Images / J. Fridrich / IEEE Workshop on Intellegent Signal Proccessing and Communication Systems. – Melbourne, Australia, 1998. – P. 173 – 177.

107. Adnan M. Watermark re-synchronization using log-polar mapping of image autocorrelation / M. Adnan, J. Meyer // Digimarc Corporation. – P. 1 – 4.

108. Ching-Yung L. Rotation, Scale, and translation resilient public watermarking for images / L. Ching-Yung, M. Wu, J.A. Bloom, M.L. Miller, I.J. Cox // IEEE Transactions on image processing. – 2000. – vol.10, No.5. – P. 767 – 782.

109. Електронні системи: навч. посіб. / Й.Й. Білинський, К.В. Огородник, М.Й. Юкиш. – В.: ВНТУ, 2011. – 109 с.

110. Грачева Ю.А. Несколько слов о стеганографии – методе защиті графической информации от нарушения авторских прав / Ю.А. Грачева // Московский государственный университет печати. – С. 76 – 81.

111. Скляр Б. Цифровая связь: Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом «Вильямс», 2007. – 1104 с.

112. Mei Jiansheng A Digital Watermarking Algorithm Based On DCT and DWT / Mei Jiansheng, Li Sukang, Tan Xiaomei // Proc. of the 2009 International Symposium on Web Information Systems and Applications. – 2009. – P. 104 – 107.

113. Ramkumar M. Data Hiding in Multimedia – Theory and Applications / M. Ramkumar // PhD tesis. – New Jersey Institute of Technology, Newark, NJ. – 2000.

114. Дьяконов В.П. Вейвлеты. От теории к практике. Изд-е 2-е. – М.: СОЛОН-Пресс, 2004. – 400 с.

115. Новиков Л.В. Основы вейвлет-анализа сигналов: учебное пособие. – СПб: ИАнП РАН, 1999. – 152 с.

116. Астафьева Н.М. Вейвлет-анализ: Основы теории и примеры применения / Н. М. Астафьева // Успехи физических наук. – 1996. – т. 166., № 11. – С. 1145 – 1170.

117. Яковлев А.Н. Введение в вейвлет-преобразования: учеб. пособие. – Новосибирск: Изд-во НГТУ, 2003. – 104 с.

118. Дьяконов В., Абраменкова И. MATLAB. Обработка сигналов и изображений. Специальный справочник. – СПб.: Питер, 2002. – 608 с.

119. Илюшин Я.А. Теория и применение вейвлет–анализа [Електронний ресурс] / Я.А. Илюшин. – Режим доступа: http://atm563.phys.msu.ru/Ilyushin/wavelet/wavelet.htm.

120. Левкович-Маслюк Л, Переберин А. Введение в вейвлет-анализ: учебный курс. – Москва: ГрафиКон’99, 1999. – 18 с.

121. Алексеев К.А. Очерк «Вокруг CWT». [Електронний ресурс] / К.А. Алексеев – Режим доступу до ресурсу: http://matlab.exponenta.ru/wavelet/book3/index.php.

122. Переберин А.В. О систематизации вейвлет-преобразований / А.В. Переберин // Вычислительные методы и программирование. – 2002. – т. 2. – с. 15 – 40.

123. Комп’ютерне моделювання систем та процесів. Методи обчислень. Частина 1: навчальний посібник / Квєтний Р.Н., Богач І.В., Бойко О.Р., Софина О.Ю., Шушура О.М.; за заг. ред. Р.Н. Квєтного. – Вінниця: ВНТУ, 2012. – 193 с.

124. Методика вейвлет-аналізу біомедичних сигналів засобами системи комп’ютерної математики MAPLE / Г.П. Чуйко, І.О. Данішевська, О.В. Дворник, С.І. Шиян // Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер.: Комп’ютерні технології. – 2013. – т. 213, вип. 201. – С. 109 – 114. – Режим доступу: http://nbuv.gov.ua/UJRN/Npchduct_2013_213_201_20

125. Zhao J. Embedding Robust Labels into Images for Copyright Protection / J. Zhao, E. Koch // In Proceedings of the International Conference on Intellectual Property Rights for Informationa, Knowledge and New Techniques. – Munchen, Wien: Oldenbourg Verlag, 1995. – P. 242 – 251.

126. Al-Haj A. Combined DWT-DCT Digital Image Watermarking / A. Al-Haj // Journal of Computer Science. – 2007. – 3(9). – P. 740 – 746.

ДОДАТОК А
АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ

ЗАТВЕРДЖУЮ

Проректор з науково-методичної роботи ХНУРЕ
к.т.н., проф.
_____ Ігнатьєв С.Є.
"__" _____ 2016 р.

АКТ
впровадження результатів дисертаційної роботи Вовк О.О. в держбюджетну НДР № 276-4 «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку»

Комісія у складі: завідувача кафедрою «Мережі зв'язку» д.т.н. Безрука В.М., доцента кафедри «Мережі зв'язку» к.т.н. Чеботарьова Д.В., відповідального виконавця НДР № 276-4 к.т.н. Кочкіна М.І. підтверджує, що ряд наукових та практичних результатів дисертаційної роботи Вовк О.О. на тему «Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації» використані в держбюджетній НДР № 276-4 «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку», що виконувалась згідно тематичного плану НДР ХНУРЕ. Зокрема, це наступні результати:

- математична модель стеганографічної системи, що дає можливість визначення оптимального методу для прихованої передачі інформації по відкритих каналах зв'язку шляхом проведення багатокритеріального аналізу;
- синтезований метод вбудовування інформації у нерухомі зображення. Завдяки використанню додаткових блоків обрізки та стійкості при попередній обробці зображення метод дозволяє отримувачу виявляти геометричні маніпуляції до детектування прихованого повідомлення.

Ці результати забезпечують надійність інфокомунікаційної системи та дозволяють підвищити імовірність правильного розпізнавання вкладених даних, навіть при наявності активного порушника.

Вказані результати використані в процесі наукових та експериментальних досліджень при виконанні НДР № 276-4 (№0113U000360), в яких автор дисертації був виконавцем.

В.М. Безрук

Д.В. Чеботарьова

М.І. Кочкін

ЗАТВЕРДЖУЮ

Проректор з науково-методичної роботи ХНУРЕ

_____ Ігнатьєв О.Є.

"18" квітня 2016 р.

АКТ

про впровадження в навчальний процес
Харківського національного університету радіоелектроніки
результатів дисертаційної роботи аспіранта кафедри «Мережі зв'язку»
Вовк Олесі Олегівни
на тему «Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації»

Комісія у складі: завідувача кафедрою «Мережі зв'язку» професора д.т.н. Безрука В.М., доцента кафедри «Мережі зв'язку» к.т.н. Золотарьова В.А., доцента кафедри «Мережі зв'язку» к.т.н. Костромицького А.І., в.о. декана факультету ТКВТ, доцента кафедри «Телекомунікаційні системи» к.т.н. Снігурова А.В., підтверджує, що результати дисертаційної роботи Вовк О.О. на тему «Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації» використовуються в навчальному процесі Харківського національного університету радіоелектроніки на кафедрі «Мережі зв'язку», а саме:

1. Наукові положення і результати дисертаційної роботи були використані при підготовці лекційних курсів із дисциплін «Захист інформації в телекомунікаційних мережах» та «Теорія електрозв'язку (ч.2)», які читаються на кафедрі «Мережі зв'язку», та «Основи стеганографічного захисту інформації», яка читається на кафедрі «Телекомунікаційні системи».

2. Програмний комплекс, що реалізовує методи вбудовування та передачі прихованої інформації ліг в основу лабораторних робіт з курсу «Основи стеганографічного захисту інформації». Метод попередньої підготовки інформації до прихованої передачі використовується в моделях телекомунікаційних систем лабораторних робіт курсу «Теорія електричного зв'язку (ч.2)».

В.М. Безрук

В.А. Золотарьов

А.І. Костромицький

А.В. Снігуров

ДОДАТОК Б
КЛЮЧОВІ ФУНКЦІЇ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СТЕГАНОГРАФІЧНИХ МЕТОДІВ НА ОСНОВІ ДКП ТА ДВП

```
using namespace std;
void Memory(double **& matr, int y, int x)
{
    matr = new double *[y];
    for (int i = 0; i < y; i++)
            matr[i] = new double[x];
}
int Block_width_count(IplImage* A, int block_size)
{
    float o;
    int w;
    o = A->width / block_size;
    trunc(o);
    w = o;
    return w;
}
int Block_height_count(IplImage* A, int block_size)
{
    float o;
    int h;
    o = A->height / block_size;
    trunc(o);
    h = o;
    return h;
}
void Dkp(double** one, double** two, int block_size)
{
    const double PI = 3.14159265358979323846;
    for (int i = 0; i < block_size; i++)
            for (int j = 0; j < block_size; j++)
                two[i][j] = 0;
    int n = block_size;
    double U, V, summ = 0;
    for (int u = 0; u < n; u++)
    {
            for (int v = 0; v < n; v++)
            {
```

```
            if (u == 0)
              U = 1 / sqrt(2);
            else U = 1;
            if (v == 0)
              V = 1 / sqrt(2);
            else V = 1;
            summ = 0;
            for (int x = 0; x < n; x++)
            {
              for (int y = 0; y < n; y++)
              {
                summ += one[x][y] * cos(PI * u * (2 * x + 1) / (2 * n)) * cos(PI * v * (2 * y + 1) / (2 * n));
              }
            }
            two[u][v] = (((U * V) / (sqrt(2 * n)))*summ);
        }
    }
}
void Odkp(double** one, double**&two, int block_size)
{
    const double PI = 3.14159265358979323846;
    int n = block_size;
    double U, V, summ = 0;
    for (int x = 0; x < n; x++)
    {
        for (int y = 0; y < n; y++)
        {
            summ = 0;
            for (int u = 0; u < n; u++)
            {
              for (int v = 0; v < n; v++)
              {
                if (u == 0) U = 1 / sqrt(2);
                else U = 1;
                if (v == 0) V = 1 / sqrt(2);
                else V = 1;
                summ += U * V *one[u][v] * cos(PI * u * (2 * x + 1) / (2 * n)) * cos(PI * v * (2 * y + 1) / (2 * n));
              }
            }
            two[x][y] = summ * (1 / (sqrt(2 * n)));
        }
    }
```

```
}
void CH_creation(double* CL, double*& CH, int N)
{
    for (int i = 0; i < N; i++)
        if (i % 2 != 0)
            CH[i] = CL[(N - 1) - i] * (-1);
        else
            CH[i] = CL[(N - 1) - i];
}
void Dwt_Out(double* data1, double*& data2, double* CL, double* CH, int delta, int N, int size, int &c)
{
    double sL; double sH;
    data2 = new double[2 * size];
    c = 0;
    for (int i = 0; i < size; i += 2)
    {
        sL = 0;
        sH = 0;
        for (int j = 0; j < N; j++)
        {
            sL += data1[(i + j - delta) % size] * CL[j];
            sH += data1[(i + j - delta) % size] * CH[j];
        }
        data2[c] = sL; c++;
        data2[c] = sH; c++;
    }
}
void Dwt_In(double*& iCL, double*& iCH, double* CL, double* CH, int N)
{
    int c = 0;
    for (int i = 0; i < N; i += 2)
    {
        iCL[c] = CL[N - i - 2];
        iCH[c] = CL[N - i - 1];
        c++;
        iCL[c] = CH[N - i - 2];
        iCH[c] = CH[N - i - 1];
        c++;
    }
}
void DWT_Off(double** one, double**&two, int x, int y, double *&CH, double *CL, double *&iCL, double *&iCH,
int N)
```

```
{
    int c;
    double *X = new double[x];
    //Переупорядочиваем столбцы и строки обратно
    for (int i = 0, h = 0; i < y / 2, h < y; i++, h += 2)
            for (int j = 0, w = 0; j < x / 2, w < x; j++, w += 2)
                two[h][w] = one[i][j];
    for (int i = y / 2, h = 1; i < y, h < y; i++, h += 2)
            for (int j = 0, w = 0; j < x / 2, w < x; j++, w += 2)
                two[h][w] = one[i][j];
    for (int i = 0, h = 0; i < y / 2, h < y; i++, h += 2)
            for (int j = x / 2, w = 1; j < x, w < x; j++, w += 2)
                two[h][w] = one[i][j];
    for (int i = y / 2, h = 1; i < y, h < y; i++, h += 2)
            for (int j = x / 2, w = 1; j < x, w < x; j++, w += 2)
                two[h][w] = one[i][j];
    CH_creation(CL, CH, N);
    Dwt_In(iCL, iCH, CL, CH, N);
    for (int i = 0; i < y; i++)
            Dwt_Out(two[i], two[i], iCL, iCH, -(y - 2), N, y, c); // -2? len(iCL)-2
    for (int i = 0; i < y; i++)
    {
            for (int j = 0; j < x; j++)
                X[j] = two[i][j];
            double* dwt_o;
            Dwt_Out(X, dwt_o, iCL, iCH, -(x - 2), N, x, c); // -2? len(iCL)-2
            for (int j = 0; j < x; j++)
                two[i][j] = dwt_o[j];
    }
}
void DWT_On(double** one, double**&two, int x, int y, double *CH, double *CL, int N)
{
    int c;
    double *X = new double[x];
    double *Y = new double[y];
    CH_creation(CL, CH, N);
    for (int i = 0; i < y; i++)
            Dwt_Out(one[i], one[i], CL, CH, 0, N, x, c);
    for (int i = 0; i < y; i++)
    {
            for (int j = 0; j < x; j++)
                X[j] = one[i][j];
```

```
            double* dwt_o;
            Dwt_Out(X, dwt_o, CL, CH, 0, N, x, c);
            for (int j = 0; j < x; j++)
                one[i][j] = dwt_o[j];
    }
    //Переупорядочиваем столбцы и строки, Низкочастотные влево и вверх, а Высокочастотные вправо и вниз
    for (int i = 0, h = 0; i < y / 2, h < y; i++, h += 2)
            for (int j = 0, w = 0; j < x / 2, w < x; j++, w += 2)
                two[i][j] = one[h][w];
    for (int i = y / 2, h = 1; i < y, h < y; i++, h += 2)
            for (int j = 0, w = 0; j < x / 2, w < x; j++, w += 2)
                two[i][j] = one[h][w];
    for (int i = 0, h = 0; i < y / 2, h < y; i++, h += 2)
            for (int j = x / 2, w = 1; j < x, w < x; j++, w += 2)
                two[i][j] = one[h][w];
    for (int i = y / 2, h = 1; i < y, h < y; i++, h += 2)
            for (int j = x / 2, w = 1; j < x, w < x; j++, w += 2)
                two[i][j] = one[h][w];
}
void Bin_1(int n, bool *b)
{
    int Q, q;
    for (int i = 0; i<8; i++)
            b[i] = 0;
    Q = n / 2;
    q = Q;
    b[7] = n % 2;
    if (Q != 0)
            while (Q != 0)
            {
                for (int i = 0; i<7; i++)
                {
                  Q = Q / 2;
                  b[6 - i] = q % 2;
                  q = Q;
                }
            }
    for (int i = 0; i<8; i++)
            cout << b[i] << " ";
    cout << endl;
    cout << endl;
};
```

```
void Bin_W(int l, int* m, bool *&Bin, int &size)
{
    bool b[8];
    size = (l + 1) * 8;
    bool *B = new bool[size];
    for (int i = 0; i<l + 1; i++)
    {
            Bin_1(m[i], b);
            for (int j = 0; j < 8; j++)
            {
                B[j + i * 8] = b[j];
            }
    }
    Bin = new bool[size];
    for (int i = 0; i < size; i++)
    {
            Bin[i] = B[i];
    }
    cout << endl << endl;
    for (int i = 0; i<size; i++)
            cout << Bin[i] << " ";
    cout << endl;
}
void Bin_txt(string text, IplImage* image, int block_size, int &bm_size, bool* &bintxt)
{
    int l = size(text);
    int *message = new int[l + 1];
    for (int i = 0; i < l; i++)
            message[i] = text[i];
    message[l] = 178;
    long block_count = (Block_width_count(image, block_size)*Block_height_count(image, block_size));
    Bin_W(l, message, bintxt, bm_size);
}
void RGB_Out(IplImage* I, double **& R, double **& G, double **& B)
{
    // пробегаемся по всем пикселям изображения
    for (int y = 0; y < I->height; y++) {
            uchar* ptr = (uchar*)(I->imageData + y * I->widthStep);
            for (int x = 0; x < I->width; x++) {
                // B - синий
                B[y][x] = ptr[3 * x];
                // G - зелёный
```

```
                G[y][x] = ptr[3 * x + 1];
                // R - красный
                R[y][x] = ptr[3 * x + 2];
            }
    }
}
void RGB_In(IplImage*& I, double **& R, double **& G, double **& B)
{
    for (int y = 0; y < I->height; y++) {
            uchar* ptr = (uchar*)(I->imageData + y * I->widthStep);
            for (int x = 0; x < I->width; x++) {
                // B - синий
                ptr[3 * x] = B[y][x];
                // G - зелёный
                ptr[3 * x + 1] = G[y][x];
                // R - красный
                ptr[3 * x + 2] = R[y][x];
            }
    }
}
void Dec_txt(string &text, bool* bintxt, int block_count)
{
    long p;
    long *M = new long[block_count / 8];
    long S[8] = { 128,64,32,16,8,4,2,1 };
    text = "Message: ";
    int length = 0;
    for (int i = 1; i < block_count / 8 + 1; i++)
    {
            p = 0;
            for (int j = 0; j < 8; j++)
            {
                p = p + ((bintxt[((i - 1) * 8) + j]) * S[j]);
                if (p == 178)
                {
                  i = block_count / 8 + 1;
                  j = 8;
                }
            }
            M[i - 1] = p; length++;
    }
    cout << "\n\nM = (" << block_count / 8 << ") ";
```

```
    for (int i = 0; i < length - 1; i++)
    {
        cout << M[i] << " ";
        text.push_back(M[i]);
    }
    cout << endl;
}
void Norm(double** one, double**& two, int y, int x)
{
    double min = one[0][0];
    for (int i = 0; i <y; i++)
        for (int j = 0; j < x; j++)
        {
            if (one[i][j] < min)
              min = one[i][j];
        }
    double max = one[0][0];
    for (int i = 0; i <y; i++)
        for (int j = 0; j < x; j++)
        {
            if (one[i][j] > max)
              max = one[i][j];
        }
    for (int i = 0; i < y; i++)
        for (int j = 0; j < x; j++)
            two[i][j] = 255 * (one[i][j] + fabs(min)) / (max + fabs(min));
}
void turn90(double** &one, int y, int x)
{
    double** two;
    Memory(two, y, x);
    for (int i = 0; i < y; i++)
        for (int j = 0; j <x; j++)
        {
            two[j][x - i - 1] = one[i][j];
        }
    for (int i = 0; i < y; i++)
        for (int j = 0; j < x; j++)
        {
            one[i][j] = two[i][j];
        }
}
```

ДОДАТОК В
МАТРИЦІ ПРІОРИТЕТІВ СТЕГАНОГРАФІЧНИХ ХАРАКТЕРИСТИК

a – пропускна здатність; *b* – стійкість; *c* – невидимість; *d* – захищеність; *e* – складність вбудовування; *f* – складність виявлення

Таблиця В.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	

Таблиця В.2

Матриця пріоритетів (для додатку захисту авторських прав на зображення, автентифікація)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/9	1/5	1/9	1/3	1/3
b	9		4	1	6	6
c	5	1/4		1/4	3	3
d	9	1	4		6	6
e	3	1/6	1/3	1/6		1
f	3	1/6	1/3	1/6	1	

Таблиця В.3

Матриця пріоритетів (для додатку відстеження порушника)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/5	1/2	1/5	3	1/4
b	5		4	1	7	2
c	2	1/4		1/4	4	1/3
d	5	1	4		7	2
e	1/3	1/7	1/4	1/7		1/6
f	4	1/2	3	1/2	6	

Таблиця В.4

Матриця пріоритетів (для додатків додавання заголовків до зображення)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/2	1	5	3	1/4
b	2		2	6	4	1/3
c	1	1/2		5	3	1/4
d	1/5	1/6	1/5		7	1/9
e	1/3	1/4	1/3	1/7		1/7
f	4	3	4	9	7	

Таблиця В.5

Матриця пріоритетів (для додатку захисту цілісності зображення)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/5	1/4	1/6	1/6	1
b	5		2	1/2	1/2	5
c	4	1/2		1/3	1/3	4
d	6	2	3		1	6
e	6	2	3	1		6
f	1	1/5	1/4	1/6	1/6	

Таблиця В.6

Матриця пріоритетів (для додатків управління копіюванням DVD записів)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/4	1/3	1/6	3	1/6
b	4		2	1/3	6	1/3
c	3	1/2		1/4	5	1/4
d	6	3	4		9	1
e	1/3	1/6	1/5	1/9		1/9
f	6	3	4	1	9	

Таблиця В.7

Матриця пріоритетів (для додатків інтелектуальних браузерів)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/5	1/3	1/6	3	1/6
b	5		3	1/2	7	1/2
c	3	1/3		1/3	5	1/3
d	6	2	3		9	1
e	1/3	1/7	1/5	1/9		1/9
f	6	2	3	1	9	

ДОДАТОК Г
МАТРИЦІ ПОРІВНЯННЯ ІСНУЮЧИХ МЕТОДІВ ЗА СТЕГАНОГРАФІЧНИМИ ХАРАКТЕРИСТИКАМИ

A1 – метод заміни найменш значущих біт; *A2* – метод Куттера-Джордана-Боссена; *A3* – метод Коха-Жао; *A4* – метод Бенгама-Мемона-Ео-Юнга; *A5* – метод із розширенням спектру; *A6* – метод, заснований на ДВП.

Таблиця Г.1

Матриця порівняння методів (за пропускною здатністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		3	7	8	5	6
A2	1/3		5	6	3	4
A3	1/7	1/5		2	1/3	1/2
A4	1/8	1/6	1/2		1/4	1/3
A5	1/5	1/3	3	4		2
A6	1/6	1/4	2	3	1/2	

Таблиця Г.2

Матриця порівняння методів (за стійкістю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		1/4	1/7	1/6	1/7	1/8
A2	4		1/4	1/3	1/4	1/5
A3	7	4		2	1	1/2
A4	6	3	1/2		1/2	1/3
A5	7	4	1	2		1/2
A6	8	5	2	3	2	

Таблиця Г.3

Матриця порівняння методів (за невидимістю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		1	3	2	1/2	1/2
A2	1		3	2	1/2	1/2
A3	1/3	1/3		1/2	1/4	1/4
A4	1/2	1/2	2		1/3	1/3
A5	2	2	4	3		1
A6	2	2	4	3	1	

Таблиця Г.4

Матриця порівняння методів (за захищеністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		1/4	1/7	1/7	1/6	1/8
A2	4		1/4	1/4	1/3	1/5
A3	7	4		1	2	1/2
A4	7	4	1		2	1/2
A5	6	3	1/2	1/2		1/3
A6	8	5	2	2	3	

Таблиця Г.5

Матриця порівняння методів (за складністю вбудовування)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		2	4	5	6	8
A2	1/2		3	4	5	7
A3	1/4	1/3		2	3	5
A4	1/5	1/4	1/2		2	4
A5	1/6	1/5	1/3	1/2		3
A6	1/8	1/7	1/5	1/4	1/3	

Таблиця Г.6

Матриця порівняння методів (за складністю вилучення)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*
A1		2	4	5	6	8
A2	1/2		3	4	5	7
A3	1/4	1/3		2	3	5
A4	1/5	1/4	1/2		2	4
A5	1/6	1/5	1/3	1/2		3
A6	1/8	1/7	1/5	1/4	1/3	

ДОДАТОК Д
МАТРИЦІ ПОРІВНЯННЯ ІСНУЮЧИХ І РОЗРОБЛЕНОГО МЕТОДУ ЗА СТЕГАНОГРАФІЧНИМИ ХАРАКТЕРИСТИКАМИ

A1 – метод заміни найменш значущих біт; *A2* – метод Куттера-Джордана-Боссена; *A3* – метод Коха-Жао; *A4* – метод Бенгама-Мемона-Ео-Юнга; *A5* – метод із розширенням спектру; *A6* – метод, заснований на ДВП.

Таблиця Д.1

Матриця порівняння методів (за пропускною здатністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		2	7	8	3	3	8
A2	1/2		5	6	3	3	6
A3	1/7	1/5		2	1/3	1/3	2
A4	1/8	1/6	1/2		1/4	1/4	1
A5	1/3	1/3	3	4		1	4
A6	1/3	1/3	3	4	1		4
A7	1/8	1/6	1/2	1	1/4	1/4	

Таблиця Д.2

Матриця порівняння методів (за стійкістю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		1/4	1/6	1/5	1/6	1/7	1/8
A2	4		1/3	1/2	1/3	1/4	1/5
A3	6	3		2	1	1/2	1/3
A4	5	2	1/2		1/2	1/3	1/4
A5	6	3	1	2		1/2	1/3
A6	7	4	2	3	2		1/2
A7	8	5	3	4	3	2	

Таблиця Д.3

Матриця порівняння методів (за невидимістю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		1	3	2	1/2	1/2	1/3
A2	1		3	2	1/2	1/2	1/3
A3	1/3	1/3		1/2	1/4	1/4	1/5
A4	1/2	1/2	2		1/3	1/3	1/4
A5	2	2	4	3		1	1/2
A6	2	2	4	3	1		1/2
A7	3	3	5	4	2	2	

Таблиця Д.4

Матриця порівняння методів (за захищеністю)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		1/4	1/6	1/6	1/5	1/8	1/8
A2	4		1/3	1/3	1/2	1/5	1/5
A3	6	3		1	2	1/3	1/3
A4	6	3	1		2	1/3	1/3
A5	5	2	1/2	1/2		1/4	1/4
A6	8	5	3	3	4		1
A7	8	5	3	3	4	1	

Таблиця Д.5

Матриця порівняння методів (за складністю вбудовування)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		2	4	5	6	7	8
A2	1/2		3	4	5	6	7
A3	1/4	1/3		2	3	4	5
A4	1/5	1/4	1/2		2	3	4
A5	1/6	1/5	1/3	1/2		2	3
A6	1/7	1/6	1/4	1/3	1/2		2
A7	1/8	1/7	1/5	1/4	1/3	1/2	

Таблиця Д.6

Матриця порівняння методів (за складністю вилучення)

	A1	*A2*	*A3*	*A4*	*A5*	*A6*	*A7*
A1		2	4	5	6	7	8
A2	1/2		3	4	5	6	7
A3	1/4	1/3		2	3	4	5
A4	1/5	1/4	1/2		2	3	4
A5	1/6	1/5	1/3	1/2		2	3
A6	1/7	1/6	1/4	1/3	1/2		2
A7	1/8	1/7	1/5	1/4	1/3	1/2	