Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Левераша Владислава Сергійовича*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне впровадження інформації в цифрові зображення за допомогою частотних методів*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
20__

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Леверашу Владиславу Сергійовичу* **академічної групи** *125м-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне впровадження інформації в цифрові зображення за допомогою частотних методів*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз основ цифрового маркування нерухомих зображень, обзор стегоалгоритмів, що ґрунтуються на ДПА, обрання методики дослідження стійкості вбудованого ЦВЗ.	03.09.2021 – 10.10.2021
Розділ 2	Дослідження взаємозалежність між коефіцієнтами ДПА та ДКП; наведено стратегію вибору частотних коефіцієнтів для вбудовування ЦВЗ; запропоновано модифікацію алгоритму цифрового маркування та оцінено його ефективність.	11.10.2021 – 24.11.2021
Розділ 3	Розрахунки капітальних витрат, витрат на модифікацію алгоритму цифрового маркування та термін окупності інвестицій застосування запропонованих рішень.	25.11.2021 – 04.12.2021

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Левераш В.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 83 с., 32 рис., 4 додатки, 32 джерела.

Об’єкт дослідження – цифрові зображення.

Предмет дослідження – алгоритми цифрового маркування графічних зображень.

Мета кваліфікаційної роботи – підвищення стійкості цифрових водяних знаків, що вбудовуються в графічні зображення, до різноманітних атак, таких як JPEG стиск, зашумлення, фільтрація та інших операцій обробки графічної інформації.

Наукова новизна результатів полягає у модифікації алгоритму, що забезпечує за рахунок вибору блоків текстур для вбудовування ЦВЗ та використання вибору частотних коефіцієнтів перетворення Адамара підвищену стійкість ЦВЗ до зашумлення зображення.

У першому розділі проаналізовано основи цифрового маркування нерухомих зображень, здійснено обзор стегоалгоритмів, що ґрунтуються на ДПА, а також обрано методику дослідження стійкості вбудованого ЦВЗ.

У спеціальній частині роботи досліджено взаємозалежність між коефіцієнтами ДПА та ДКП; наведено стратегію вибору частотних коефіцієнтів для вбудовування водяного знаку; запропоновано модифікацію алгоритму цифрового маркування та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на модифікацію алгоритму цифрового маркування та термін окупності інвестицій застосування запропонованих рішень.

ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, СТЕГАНОГРАФІЯ, КОМПРЕСІЯ, ЗОБРАЖЕННЯ-КОНТЕЙНЕР, ОРТОГОНАЛЬНЕ ПЕРЕТВОРЕННЯ, ГРАФІЧНИЙ ФАЙЛ, ЧАСТОТНА ОБЛАСТЬ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка 83 с., 32 рис., 4 приложения, 32 источника.

Объект исследования – цифровые изображения.

Предмет исследования – алгоритмы цифровой маркировки графических изображений.

Цель квалификационной работы – повышения устойчивости цифровых водяных знаков, встраиваемых в графические изображения, к различным атакам, таким как JPEG сжатие, зашумление, фильтрация и другие операции обработки графической информации.

Научная новизна результатов заключается в модификации алгоритма, обеспечивающего за счет выбора блоков текстур для встраивания ЦВЗ и использования выбора частотных коэффициентов преобразования Адамара повышенную стойкость ЦВЗ к зашумлению изображения.

В первой главе проанализированы основы цифровой маркировки неподвижных изображений, осуществлен обзор стегоалгоритмов, основанных на ДПА, а также избрана методика исследования устойчивости встроенного ЦВЗ.

В специальной части работы исследована взаимозависимость между коэффициентами ДПА и ДКП; приведена стратегия выбора частотных коэффициентов для встраивания водяного знака; предложена модификация алгоритма цифровой маркировки и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, затрат на модификацию алгоритма цифровой маркировки и сроки окупаемости инвестиций применения предложенных решений.

ЦИФРОВОЙ ВОДЯННЫЙ ЗНАК, СТЕГАНОГРАФИЯ, КОМПРЕССИЯ, ИЗОБРАЖЕНИЕ-КОНТЕЙНЕР, ОРТОГОНАЛЬНОЕ ПРЕОБРАЗОВАНИЕ, ГРАФИЧЕСКИЙ ФАЙЛ, ЧАСТОТНАЯ ОБЛАСТЬ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 83, fig. 32, 4 additions, 32 sources.

The object of research is digital images.

The subject of research – algorithms for digital marking of graphic images.

The purpose of the qualification work is to increase the resilience of digital watermarks embedded in graphic images to various attacks, such as JPEG compression, noise, filtering and other graphic information processing operations.

The scientific novelty of the results lies in the modification of the algorithm, which provides increased resistance of the digital watermark to image noise by selecting texture blocks for digital watermark embedding and using the choice of Hadamard frequency conversion factors.

The first section analyzes the basics of digital marking of still images, reviews stegoalgorithms based on discrete Hadamard transform, and selects a method for studying the stability of the built-in digital watermark.

In the special part of the work the interdependence between the coefficients of discrete Hadamard transformation and discrete cosine transformation is investigated; the strategy of selection of frequency coefficients for embedding a digital watermark is given; a modification of the digital marking algorithm is proposed and its efficiency is evaluated. Based on the results of research, conclusions were made regarding the solution of the problem.

In the economic section, calculations of capital costs, costs of modifying the digital labeling algorithm and the payback period of investments in the application of the proposed solutions are performed.

DIGITAL WATERMARK, STEGANOGRAPHY, COMPRESSION, IMAGE-CONTAINER, ORTHOGONAL TRANSFORMATION, GRAPHIC FILE, FREQUENCY, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

БЧХ – Боуза-Чоудхурі-Хоквінгема;

ДВП – Дискретне вейвлет перетворення;

ДКП – Дискретне косинусне перетворення;

ДПА – Дискретне перетворення Адамара;

ДПФ – Дискретне перетворення Фур'є;

ДПХ – Дискретне перетворення Хаара;

ДСП – Дискретне синусне перетворення;

ЕЦП – Електронний цифровий підпис;

ЗСЛ – Зорова система людини;

ПВП – Псевдовипадкова послідовність;

ПКЛ – Перетворення Карунена-Лоєва;

ЦВЗ – Цифровий водяний знак;

PSNR – Peak Signal to Noise Ratio – Пікове відношення сигналу до шуму.

ЗМІСТ

ВСТУП

Інтерес до стеганографії з'явився останні десятиліття і викликаний широким поширенням мультимедійних технологій. Методи стеганографії дозволяють не лише приховано передавати дані, але й вирішувати завдання завадостійкої аутентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації по мережах зв'язку, пошуку інформації в мультимедійних базах даних.

Отже, стеганографія – наука, що швидко й динамічно розвивається, використовує методи і досягнення криптографії, цифрової обробки сигналів, теорії зв'язку та інформації [1].

Одним з напрямків стеганографії є цифрове маркування, яке здійснює непомітне вбудовування в об'єкт захисту невидимою для людського ока цифровий мітки – цифрового водяного знаку (ЦВЗ) [1-3]. Наявність вбудованого в об'єкт захисту ЦВЗ дозволяє однозначно визначити автора документа, що утримує потенційного зловмисника від незаконного поширення мультимедійної інформації.

З розвитком обчислювальної техніки широкого поширення набули комп'ютеризовані системи електронного документообігу. Електронний архів – це окремий випадок системи документообігу, орієнтований на ефективне зберігання та пошук інформації. За допомогою електронного архіву можна поєднати всі форми даних – документи, Web, нерухомі зображення та аудіовізуальну інформацію – у різних робочих процесах та додатках [4].

Для аутентифікації інформації у системах електронного документообігу застосовується електронний цифровий підпис (ЕЦП). Однак відомі системи ЕЦП не забезпечують захист авторства не тільки цифрових, а й аналогових повідомлень в умовах, коли активний порушник вносить спотворення в повідомлення, що захищається, і аутентифікуючу інформацію [5]. Частково цих недоліків позбавлений ЦВЗ. Однак наразі існує досить велика кількість шкідливих впливів, які зловмисники можуть використовувати для видалення

вбудованого в графічний файл ЦВЗ з метою унеможливлення визначення джерела витоку інформації. Прикладами таких шкідливих впливів є: зашумлення, фільтрація, зміна розміру та яскравості. Застосовуючи ці атаки, зловмисник може значно ускладнити процес відстеження незаконного копіювання інформаційних ресурсів.

У зв'язку з глобальним розповсюдженням Інтернету велику поширеність отримав формат JPEG, що дозволяє здійснювати ефективне стиснення зображень, не викликаючи сильних видимих спотворень. Використовуючи JPEG компресію, зловмисники здатні знищити вбудований в зображення водяний знак, зберігши при цьому комерційну якість зображення. Незважаючи на те, що наразі існує більш ефективний формат стиснення JPEG2000, формат JPEG зберігає свої лідируючі позиції.

Таким чином, дослідження та удосконалення алгоритмів цифрового маркування нерухомих зображень, стійких до компресії JPEG та інших шкідливих впливів, наразі є актуальною задачею.

Метою роботи є підвищення стійкості цифрових водяних знаків, що вбудовуються в графічні зображення, до різноманітних атак, таких як JPEG стиск, зашумлення, фільтрація та інших операцій обробки графічної інформації.

Постановка задачі:

• аналіз технологій цифрового маркування графічних зображень у частотній області;

• обґрунтування вибору типу ортогонального перетворення;

• вибір критеріїв з метою оцінки ефективності алгоритмів цифрового маркування, здатного протистояти різноманітним атакам;

• проведення аналізу впливу JPEG стиснення на частотні коефіцієнти обраного ортогонального перетворення;

• дослідження та удосконалення алгоритмів цифрового маркування, які забезпечують стійкість ЦВЗ до різноманітних атак.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Цифрове маркування нерухомих зображень

1.1.1 Місце цифрового маркування у стеганографії

Стеганографія має декілька напрямків: класичний, комп'ютерний і цифровий.

Основне призначення класичної стеганографії – приховування інформації. Класична стеганографія зародилася дуже давно. Перші згадки датуються V ст. до н.е. в історичних працях Геродота.

З появою комп'ютерів з'явилося два нових напрямки у стеганографії: комп'ютерний та цифровий. Основне призначення комп'ютерної стеганографії – прихована передача даних. Вона включає безліч методів, що використовують комп'ютерні формати даних, особливості файлової системи, сектори, що не використовуються тощо.

Найбільшого поширення набули методи, що використовують цифрову обробку сигналів – цифрова стеганографія, яка має декілька напрямків використання [1, 7]:

• вбудовування інформації в цифровий носій з метою його прихованої передачі;

• вбудовування ідентифікаційних номерів;

• приховане анотування документів;

• цифрове маркування мультимедійної продукції.

Отже, для захисту мультимедійної продукції використовуються цифрове маркування і вбудовування ідентифікаційних номерів.

Наразі вбудовування ЦВЗ – один з найефективніших методів захисту зображень від незаконного розповсюдження. Цифрове маркування налічує велику кількість алгоритмів, що мають різний рівень ефективності. На рис. 1.1 представлені сфери застосування ЦВЗ [1, 7].

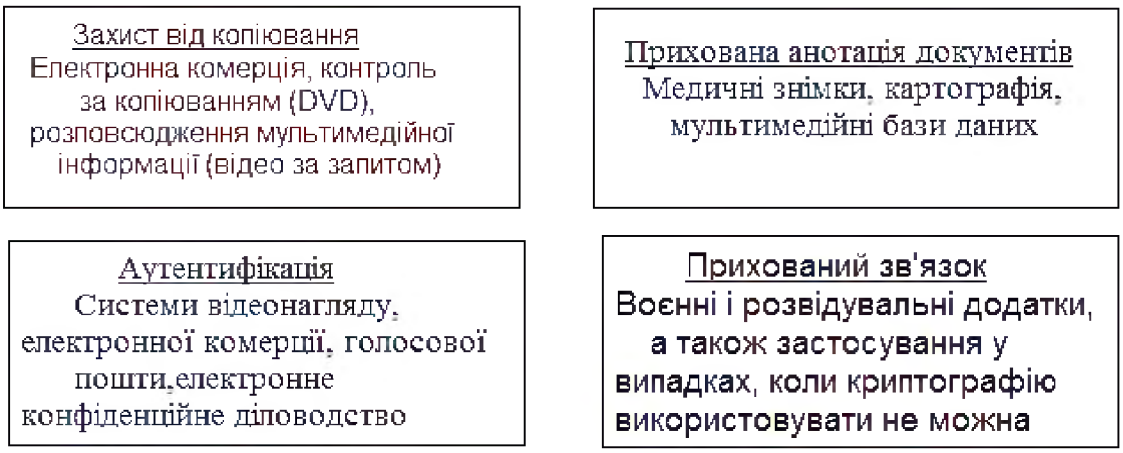


Рисунок 1.1 – Області застосування цифрового маркування

Отже, вбудовування ЦВЗ є одним із методів цифрової стеганографії. Даний напрямок чудово підходить для вирішення завдань запобігання незаконному копіюванню та модифікації мультимедійної інформації, захисту авторських прав.

1.1.2 Основні поняття стеганографії

Основні визначення сучасної стеганографії було прийнято у 1996 р. на конференції Information Hiding: First Information Workshop [8]. Розглянемо дані поняття стосовно області цифрового маркування мультимедійної інформації.

У стеганографії існує кілька різновидів контейнерів [1, 6-8]:

• контейнер – будь-яка інформація, призначена для приховування у ній таємних повідомлень;

• порожній контейнер – контейнер без вбудованого повідомлення;

• стегоконтейнер – заповнений контейнер, що містить вбудовану інформацію.

Контейнером може бути текст, нерухоме зображення, аудіо або відеоінформація. Останні три типи контейнерів використовуються найчастіше.

У свою чергу контейнер поділяється на фіксований (наприклад, зображення) і потоковий (наприклад, телефонну розмову). Найбільшого

поширення набули дослідження з використанням фіксованого контейнера, оскільки при виборі потокового контейнера дослідник стикається з проблемою синхронізації ЦВЗ з контейнером, визначення його початку та кінця [1].

Вбудоване (приховане) повідомлення – повідомлення, що вбудовується у контейнер. У цьому випадку таким вбудованим повідомленням і є ЦВЗ.

Стеганографічний канал (стегоканал) – канал передачі стегоконтейнера [6-8]. Характеризується пропускною спроможністю, що визначає граничний обсяг вбудованої інформації.

Стегоключ (ключ) – секретний ключ, що використовується для приховування інформації та її подальшого вилучення [8]. Не знаючи стегоключ, неможливо визначити місце розташування вбудованого в контейнер ЦВЗ. Стегоключ є невід'ємним елементом будь-якої стеганографічної системи.

Стеганографічна система (стегосистема) – сукупність засобів та методів, що використовуються для формування прихованого каналу передачі інформації [8]. На рис. 1.2 представлено узагальнену схему цифрового маркування [1, 6].

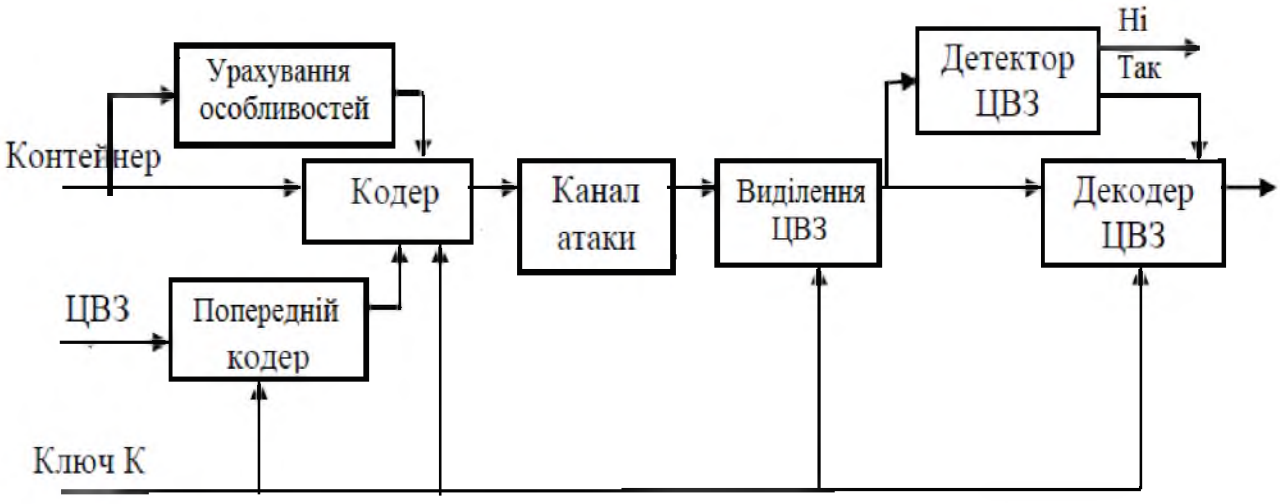


Рисунок 1.2 – Схема типової стегосистеми цифрового маркування

На вхід системи надходить контейнер та ЦВЗ. Перед операцією вбудовування враховуються особливості контейнера, наприклад клас зображення та його формат (у разі використання зображення як контейнер), а

ЦВЗ піддається попередній обробці у попередньому кодері. Прикладом попередньої обробки ЦВЗ може бути використання дискретного перетворення Фур'є, дискретного вейвлет-перетворення і т.д. Після попередніх операцій у пристрої-кодері за заданим алгоритмом здійснюється вбудовування ЦВЗ у контейнер. Стегоконтейнер може передаватися певним каналом, при цьому піддаючись атакам різного типу.

Виділення ЦВЗ може відбуватися у два етапи. Пристрій-детектор ЦВЗ, керуючись певним критерієм, визначає наявність ЦВЗ у прийнятій інформації. При цьому стегосистемі може бути потрібний початковий контейнер (закриті стегосистеми), або не потрібний (сліпі стегосистеми). У разі наявності водяного знака застосовується пристрій-декодер, який витягує ЦВЗ за певним алгоритмом. Варто зазначити, що детектором додатково може виступати й людина. Тому при розробці алгоритмів цифрового маркування обов'язково повинні враховуватися особливості слухової та зорової системи людини (ЗСЛ).

1.1.3 Методи нанесення цифрових водяних знаків

Наразі існує безліч способів вбудовування ЦВЗ, які можна розділити на три класи: просторові, частотні та засновані на моментах [9].

Просторові методи нанесення водяних знаків оперують значеннями кольору або яскравістю пікселів зображення, отже не вимагають складних розрахунків і перетворень контейнера. Вбудовування ЦВЗ проводиться [9]:

- безпосередньо в біти кольору (методи найменшого біта, метод псевдовипадкової послідовності (ПВП), алгоритм Куттера-Джордона);
- за рахунок зміни яскравостей пікселів або блоків зображення (метод блокового приховування, алгоритм Пітаса, алгоритм Лангелара);
- безпосередньо на палітру зображення (метод заміни палітри);
- за допомогою клонування подібних за статистичними оцінками блоків самого ЦВЗ та оригіналу (алгоритм Бендера).

Використання та вилучення водяного знака у просторових методах здійснюється як за допомогою точних залежностей, так і за допомогою статистичних оцінок, які мають деяку похибку вірного виявлення мітки.

Недоліками даної групи методів є погана стійкість до різних операцій над зображенням, зокрема після стиснення контейнера будь-який просторовий метод не може гарантувати збереження водяного знака [9]. Зумовлено це подібним характером впливу процесів нанесення ЦВЗ та стиснення зображення, оскільки обидва процеси беруть за основу принцип візуальної надмірності цифрової інформації. До переваг просторових методів відносяться простота реалізації та відсутність складних обчислень для підготовки контейнера та знака.

Методи, засновані на моментах зображення, є малопоширеною групою методів через невисокий виграш у стійкості ЦВЗ щодо обчислювальних витрат. Алгоритми цієї області засновані на ймовірності моделі зображень, і вбудовування водяного знака проводиться в моменти зображень. Моменти є дескрипторами (описами) особливостей зображення. За основу такі алгоритми приймають перетворення, відомі як моменти Чебишева, Лежандра чи Зернік [9]. Мала кількість наукової літератури з цієї тематики явно вказує на те, що ці методи не потрібні і застосовуються в окремих випадках, оскільки проблема стійкості в них вирішується лише частково, а обчислювальні витрати на перетворення зображення досить великі.

Частотні методи засновані на перетвореннях частотної області зображення. Їх висока робастність обумовлена перерозподілом енергії знака і контейнера таким чином, щоб помістити ЦВЗ у найбільш значущі області зображення, які не зачеплять стиснення. За допомогою перетворень здійснюється декомпозиція зображення на низькочастотні та високочастотні області представлені спектральними коефіцієнтами. Саме з допомогою маніпуляцій цими коефіцієнтами здійснюється використання водяного знака. Далі зміненим значенням спектральних коефіцієнтів застосовується зворотне перетворення, і на виході отримують маркіроване зображення.

До частотних перетворень відносять:

• дискретне перетворення Фур'є (ДФП);

• дискретне косинусне (дискретне синусне) перетворення (ДКП і ДСП);

• дискретне вейвлет перетворення (ДВП);

• дискретне перетворення Адамара (ДПА);

• перетворення Карунена-Лоєва (ПКЛ) та інші.

Таким чином, перевагами частотних методів є стійкість до компресії зображення та шуму. До недоліків відноситься велика обчислювальна складність і слабка стійкість до геометричних атак. Виходячи з теми даної роботи і ґрунтуючись на перевагах частотних методів, як спосіб вбудовування ЦВЗ було обрано алгоритми даного класу.

1.1.4 Вимоги, що висуваються до алгоритмів цифрового маркування

Існує ряд обов'язкових вимог, що пред'являються до цифрових стеганографічних алгоритмів, основними з яких є [1, 7]:

• стійкість (робастність);

• невиявлення;

• невидимість.

Стійкість стеганографічного алгоритму полягає у здатності ЦВЗ зберігати свій первісний вид після впливу на стегоконтейнер атак різного типу.

Невиявлення полягає у здатності протистояти різним методам стегоаналізу: [10-14], які використовує стегоаналітик для виявлення факту присутності ЦВЗ у контейнері.

Невидимість характеризується здатністю алгоритму не вносити видимих людським оком змін у зовнішній вигляд контейнера. Отже, як зазначалося у розділі 1.1.2, необхідно враховувати особливості ЗСЛ, які поділяються на дві категорії [1]:

• низькочастотні, до яких відносяться чутливість людського ока до змін яскравості зображення, його частотної складової, а також ефекту маскування;

• високочастотні, що проявляються в підстроюванні мозком низькочастотних властивостей під зображення (наприклад, чутливість контрасту, розміру, формі, кольору, розташування окремих об'єктів тощо).

Варто зазначити, що надійність стегосистеми залежить від обсягу вбудованого ЦВЗ. Отже, необхідне дотримання компромісу між рівнем надійності вбудовування та обсягом ЦВЗ. На рис. 1.3 відображено цю залежність при постійному розмірі контейнера [3].

Рисунок 1.3 – Залежність стійкості стегосистеми від обсягу вбудованого ЦВЗ

Слід зауважити, що крім перерахованих вище вимог стеганографічний алгоритм повинен мати прийнятну обчислювальну складність.

1.1.5 Класифікація атак на системи цифрового маркування

Серед великої кількості робіт, присвячених класифікації атак зловмисників на системи цифрового маркування, найповніша наведена в [15], схема з якої відображена на рис. 1.4.

Згідно з цією класифікацією всі атаки проти систем цифрового маркування можна розділити на два класи: системні атаки та неавторизований вплив.

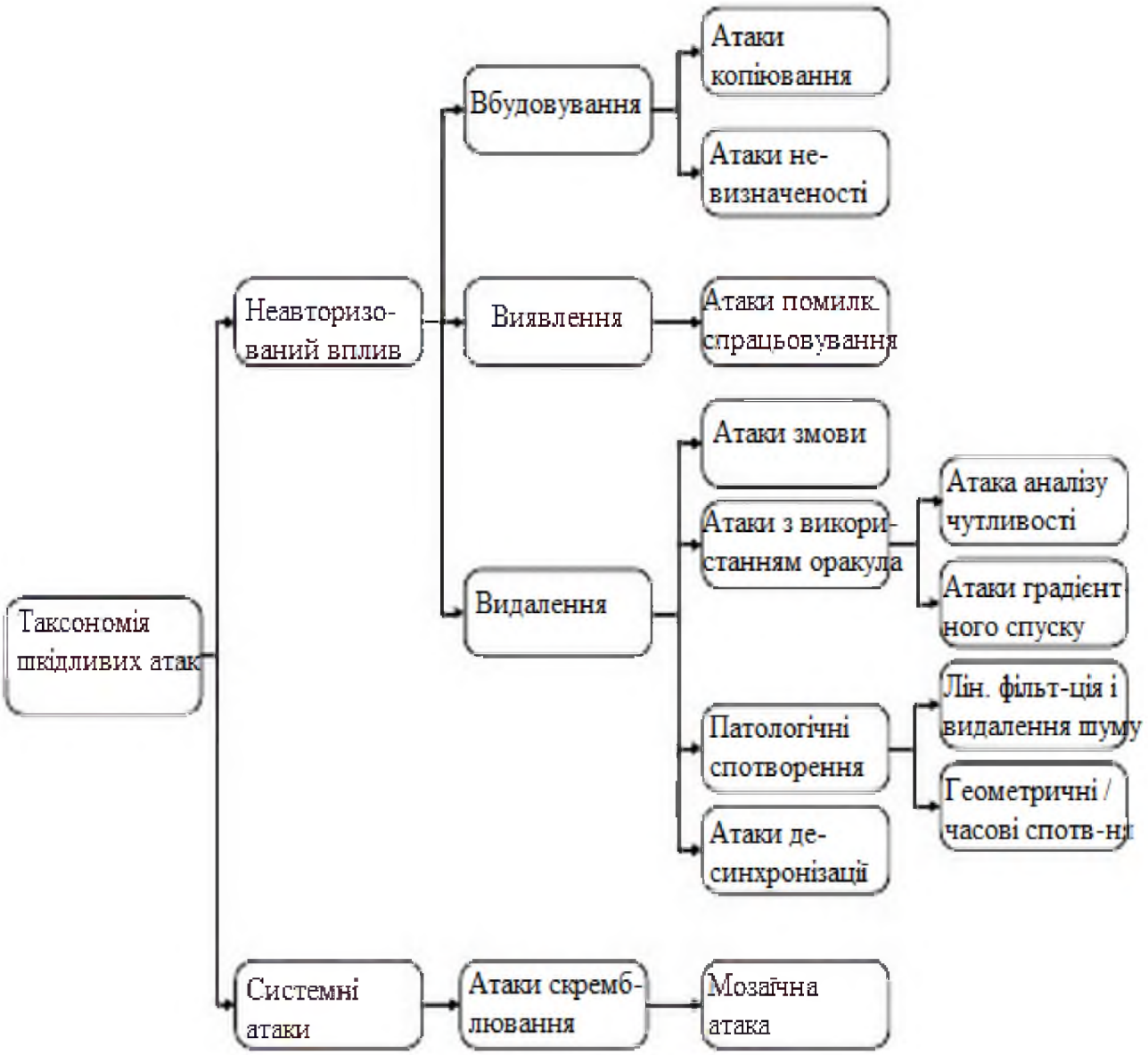


Рисунок 1.4 – Класифікація атак на системи цифрового маркування

Системні атаки використовують помилки у роботі стегосистеми. Прикладом шкідливого впливу цього типу є мозаїчна атака, що застосовується в мережі Інтернет. При використанні мозаїчної атаки стегоконтейнер розбивається на окремі фрагменти, які надто малі, щоб зберігати у собі ЦВЗ. На сторінці Інтернет-сайту ці фрагменти розміщуються поруч один з одним, візуально утворюючи початкове зображення.

Атаки неавторизованого впливу використовують уразливості в системі цифрового маркування і в свою чергу поділяються на атаки неавторизованого вбудовування, виявлення і видалення ЦВЗ відповідно.

При неавторизованому вбудовуванні зловмисник вбудовує свій ЦВЗ в стеганографічний контейнер.

Атаки неавторизованого виявлення спрямовані на встановлення факту присутності ЦВЗ в стегоконтейнері або на імітацію присутності ЦВЗ в контейнері (атака помилкового спрацьовування) при наявності детектора у зловмисника.

Використовуючи атаки неавторизованого видалення, зловмисник прагне повністю видалити ЦВЗ з стегоконтейнера (наприклад, лінійна фільтрація) або зробити водяний знак невидимим для детектора (геометричні атаки).

Одним з найпоширеніших шкідливих впливів на системи цифрового маркування є компресія зображення у зв'язку з широким розповсюдженням в мережі Інтернет графічного формату JPEG, а також більш ефективного формату JPEG2000, що набирає популярність. Тому в рамках цієї роботи основну увагу було приділено дослідженню протидії систем цифрового маркування атакам компресії зображення.

1.1.6 Особливості атаки компресії зображення

Компресія зображення належить до класу атак, спрямованих на видалення ЦВЗ зі стегоконтейнера, у яких ЦВЗ сприймається як статистичний шум [1]. Найбільш поширеними алгоритмами стиснення зі втратами є JPEG та JPEG2000. Ці алгоритми ґрунтуються на застосуванні дискретних ортогональних перетворень.

Основою JPEG-стиснення є ДКП. Початкове зображення розбивається на ряд блоків розміром 8x8 пікселів. Кожен блок піддається ДКП для перерозподілу енергії зображення. В результаті виходить набір матриць коефіцієнтів ДКП, кожну з яких становить низькочастотний коефіцієнт DC (верхній лівий коефіцієнт матриці) та високочастотні коефіцієнти AC. Кожна матриця коефіцієнтів піддається квантуванню за допомогою наперед заданої таблиці квантування. При цьому обнулюється більша частина високочастотних

коефіцієнтів. Кожна отримана матриця квантованих коефіцієнтів перетворюється на одномірний вектор, який містить довгі послідовності нулів, що дозволяє ефективно використовувати на завершальній стадії JPEG-компресії RLE-стиснення (кодування довжин серій) і стиснення по Хафману.

Основою стиснення JPEG2000 є ДВП, яке здійснює перерозподіл енергії зображення. На відміну від JPEG стиснення вейвлет-перетворення застосовується до всього зображення повністю. Основна ідея вейвлет-перетворення сигналу полягає в ієрархічному розкладанні вхідного сигналу на послідовності так званих базових компонент з розрідженням, яке послідовно зменшується, і пов'язаних з ним компонент деталей [16]. У порівнянні з ДКП ДВП має набагато кращу здатність перерозподіляти енергію зображення.

Як видно з опису алгоритмів, JPEG і JPEG2000 використовують дискретні ортогональні перетворення для перерозподілу енергії зображення з подальшим знищенням інформації у першу чергу в високочастотних субсмугах, що необхідно враховувати при вбудовуванні ЦВЗ в контейнер.

1.1.7 Вибір перетворення для вбудовування ЦВЗ у частотну область зображення-контейнера

Для застосування ЦВЗ у частотній області необхідно правильно вибрати відповідне перетворення.

Дискретні ортогональні перетворення можна порівнювати за виграшом від кодування, під яким розуміється ступінь перерозподілу дисперсій коефіцієнтів перетворення. На рис. 1.5 представлені деякі перетворення відповідно до величини виграшу від кодування, де найбільший виграш дає ПКЛ, а найменший – розкладання базисом одиничного імпульсу (тобто відсутність перетворення) [1].

У алгоритмах цифрового маркування бажано, щоб перетворення, яке використовується, враховувало особливості формату стиснення зображення.

Тому найчастіше використовуються ДКП [17] та ДВП [18], оскільки вони застосовуються у форматах стиснення JPEG та JPEG2000, відповідно.

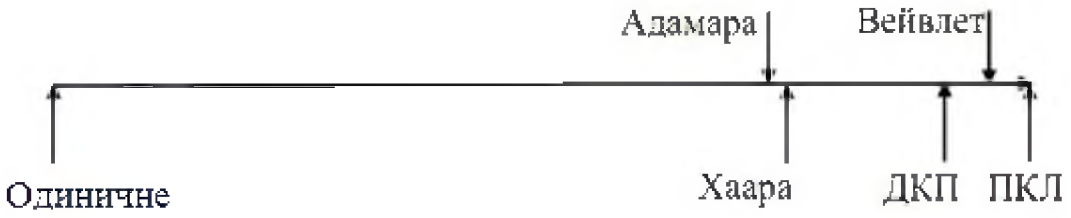


Рисунок 1.5 – Розподіл деяких перетворень відповідно до виграшу від кодування

Однак необхідно враховувати, що алгоритми, що базуються на ДКП, можуть бути нестійкими до низькорівневої компресії JPEG2000, заснованої на ДВП і навпаки [1].

В останні роки в частотних алгоритмах цифрового маркування застосовується ДПА, яке для додаткового зменшення обчислювальної складності визначається рядково-стовпцевим чином:

$$F_N = \frac{1}{N} A_N \left[X_N A_N \right], \tag{1.1}$$

де N – порядок матриці Адамара; A_N – ядро перетворення Адамара, рядки якого представлені послідовністю 1 та -1; X_N – матриця пікселів зображення; F_N – матриця частотних коефіцієнтів.

Матриця ядра ДПА має властивість симетричності, тобто:

$$A_N = A_N^T. \tag{1.2}$$

Чим більша кількість змін знаку у рядку ядра ДПА, тим більша частотність коефіцієнта. Ядро ДПА порядку $N=2^n$, де n – ціле позитивне число, яке формується за допомогою операції кронекерівського множення матриць:

$$A_{2N} = A_2 \otimes A_N = \begin{bmatrix} A_N & A_N \\ A_N & -A_N \end{bmatrix}, \tag{1.3}$$

де $A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ є матрицею Адамара найменшого порядку.

Слід зазначити, що використання цього перетворення забезпечує схожу із ДКП стійкість ЦВЗ до шкідливих впливів, в окремих випадках навіть перевищуючи її.

Отже, крім ДКП і ДВП велику перспективу має й ДПА, що обумовлено наступними чинниками [19]:

• низькою обчислювальною складністю порівняно з ДКП та ДВП;

• здатністю протистояти високому рівню компресії незалежно від використовуваної платформи стиснення (JPEG або JPEG2000);

• потенційною можливістю вбудовувати ЦВЗ більшого обсягу, ніж алгоритми на основі ДКП та ДВП, оскільки для підвищення обсягу ЦВЗ, що вбудовується в контейнер, краще застосовувати перетворення з меншими виграшами від кодування, які погано підходять для стиснення сигналів;

• низьким рівнем спотворень, що вносяться при вбудовуванні ЦВЗ, порівняно з алгоритмами, заснованими на використанні ДКП і ДВП;

• простотою апаратної реалізації.

Отже, з перелічених вище положень в рамках цієї роботи було вирішено для впровадження ЦВЗ в нерухомі зображення обрати саме перетворення Адамара.

1.2 Огляд стеганографічних алгоритмів, що ґрунтуються на перетворенні Адамара

Було розглянуто основні аспекти деяких алгоритмів цифрового маркування, заснованих на перетворенні Адамара. Слід відзначити, що за рахунок використання даного перетворення всі аналізовані алгоритми мають відносно низьку обчислювальну складність.

Алгоритм Maity [19] для вбудовування ЦВЗ використовує ДПА. ЦВЗ може бути або багатозначним напівтоновим зображенням, або послідовністю

біт. Для оптимального приховування ЦВЗ автори використовували особливості ЗСЛ, що на їх думку було застосовано вперше для перетворення Адамара. Алгоритм Maity має стійкість до атак видалення водяного знаку, забезпечує хорошу стійкість до стиснення JPEG та JPEG2000. Недоліком алгоритму Maity є необхідність наявності інформації про коефіцієнти перетворення контейнера та їх місцезнаходження.

Алгоритм Santi [20], як і алгоритм Maity заснований на застосуванні ДПА. ЦВЗ є бінарним зображенням, впровадження якого здійснюється в низько-інформативні та середньо-інформативні блоки ДПА контейнера. Для підвищення стійкості алгоритму до компресії використано адаптивну негативну модуляцію. Перевагою алгоритму Santi є висока стійкість до компресії високого рівня JPEG та JPEG2000 та до інших загальних операцій обробки зображення. Недоліком алгоритму Santi є необхідність наявності додаткової інформації про місцезнаходження ЦВЗ у стегоконтейнері.

Алгоритм Anthony [21] ґрунтується на швидкому перетворенні Адамара. Як ЦВЗ використовується напівтонове зображення-логотип. Алгоритм є сліпою стеганографічною схемою. Алгоритм має відносну стійкість до JPEG-стиснення, обрізання рівня 50% і деяким іншим атакам. Однак алгоритм Anthony має ряд недоліків: слабку стійкість до середньочастотної фільтрації 2×2 і гаусової фільтрації 3×3, до обрізування рівня 75% і JPEG стиску з коефіцієнтом якості менше 30.

В основі алгоритму Saeid [22] лежить перетворення Адамара, яке вбудовує у контейнер напівтонове зображення. Контейнер розбивається на блоки розміром 4×4. Два прилеглі низькочастотні коефіцієнти АС перетворення Адамара кожного блоку контейнера піддаються модифікації на підставі значень DC-коефіцієнтів прилеглих блоків розміром 8×8. Алгоритм Saeid є сліпим. Має стійкість до атаки «солі і перцю», корекції гістограми, середньочастотної фільтрації 3×3, а також JPEG стиску до рівня стиснення 50%. Недоліком алгоритму Saeid є недостатньо висока стійкість до компресії високого рівня.

Алгоритм Разінкова [23] заснований на застосуванні мультирозширеного та комплексного перетворення Адамара. Для усунення похибки вбудовування низькочастотні коефіцієнти мультирозширеного перетворення Адамара збільшуються на певну величину. За допомогою комплексного перетворення Адамара послідовність біт (ЦВЗ) ховається в низькочастотній області контейнера. Алгоритм є сліпим і стійким до таких атак, як зменшення зображення (до 53% від початкових розмірів), поворот зображення на кут до 15 градусів, JPEG-компресії зі збереженням 25% якості зображення.

Алгоритм Zhang [24] заснований на використанні перетворення Адамара, що реалізується рядково-стовпцевим методом, який автор називає швидким двомірним ДПА. В алгоритмі Zhang ЦВЗ (монохромне чорно-біле зображення) піддається скремблюванню. Контейнер розбивається на блоки, що не перекриваються, розміром 8×8. Вбудовування біта водяного знаку ґрунтується на зміні співвідношення величин заданих пар коефіцієнтів ДПА обраних блоків зображення. Алгоритм Zhang має погану скритність через велику кількість артефактів стегоконтейнера, які утворюються. Опірність JPEG стиску слабка – помітні спотворення ЦВЗ спостерігаються вже за коефіцієнті якості Q=60.

Алгоритм Latif [25] впроваджує в блоки контейнера, які неперекриваються, і є розміром 8×8, бінарне чорно-біле зображення з використанням похилого параметричного перетворення Адамара. Перевагою алгоритму Latif є необхідність використання контейнера для вилучення ЦВЗ. Недоліками є неприпустимо-високий рівень спотворень зображення та слабка стійкість до стиску JPEG.

Інший алгоритм Anthony [26] призначений для супутникових зображень. Алгоритм заснований на двомірному рядково-стовпцевому перетворенні Адамара. Початковим ЦВЗ є рядок символів. Вбудовування водяного знаку здійснюється в блоки контейнера, що не перекриваються, розміром 8×8. Відмінною особливістю алгоритму є використання коригувальних кодів БЧХ (Боуза-Чоудхурі-Хоквінгема) при вбудовуванні ЦВЗ. Використання кодів БЧХ

підвищує стійкість ЦВЗ. Алгоритм Anthony [26] забезпечує дуже високу скритність ЦВЗ.

Особливу увагу було приділено дослідженню алгоритмів [27-29].

Алгоритм Sarker [27] використовує двомірне рядково-стовпцеве ДПА. Як ЦВЗ використовується монохромне чорно-біле зображення. Як і більшість алгоритмів цифрового маркування, вбудовування ЦВЗ здійснюється в блоки контейнера розміром 8×8. До вибраних блоків застосовується ДПА. В отриманому блоці частотних коефіцієнтів за допомогою алгоритму пошуку за першим найкращим збігом здійснюється пошук найдовшого графа з найбільшим останнім частотним коефіцієнтом, в який здійснюється вбудовування ЦВЗ. Алгоритм Sarker демонструє хорошу стійкість до JPEG стиску, фільтрації та зашумлення. Проте спотворення зображення після вбудовування ЦВЗ помітні. Крім того, вбудовуванню підлягає не весь ЦВЗ, а коефіцієнти, модуль яких менше 1. Інші коефіцієнти водяного знаку використовуються як ключ. Однак на практиці використання такого алгоритму неможливе. Якщо детектор має суттєву інформацію про ЦВЗ, вона повинна бути використана лише для визначення присутності водяного знаку в стегоконтейнері, але не для вилучення. Тому алгоритм Sarker не є коректним.

Алгоритм Bhatnagar [28] використовує мультидозвільне перетворення Адамара, яке аналогічне вейвлет-перетворенням. Початкове зображення розкладається на ряд рівнів розкладання. Високочастотні коефіцієнти піддаються сингулярному розкладанню за формулою:

$$A=U\times S\times V'; \qquad (1.4)$$

де U і V – ортогональні матриці; S – діагональна матриця сингулярних чисел, коефіцієнти діагоналі якої розташовані в порядку зменшення.

Сингулярному розкладу також піддається й ЦВЗ. Його матриці U_w і V_w використовуються як ключ для отримання водяного знаку. Матриця S_w вбудовується в матрицю контейнера S.

Алгоритм Bhatnagar демонструє високий рівень непомітності вбудованої інформації та велику стійкість до JPEG компресії, зашумлення високого рівня,

фільтрації та інших атак. Однак цей алгоритм, як і алгоритм Sarker [27] не може бути використаний на практиці, оскільки впровадженню підлягає лише частина інформації ЦВЗ, а саме – набір сингулярних коефіцієнтів матриці S_w. Подібний підхід може призвести до помилки помилкового спрацьовування, і ЦВЗ може бути вилучений із зображення, в якому він не знаходиться.

На рис. 1.6,а-б представлено два зображення. Піддамо обидва ці зображення сингулярному розкладанню. Сингулярні числа S_{w1} і S_{w2} обох зображень сильно відрізнятимуться. Нехай сингулярні числа зображення (рис. 1.6,б) були вилучені із зображення, в яке не було вбудовано ЦВЗ (рис. 1.6,а). Використаємо матриці U_{w1} та V_{w1} зображення з рис. 1.6,а як ключ. Відновимо ймовірно вилучений ЦВЗ, використовуючи сингулярні числа S_{w2}. Перетворимо отримане зображення на бінарне (рис. 1.6,в).

а б в

Рисунок 1.6 – Приклад помилкового спрацьовування детектора:
а – початковий ЦВЗ, б – зображення із випадковим розташуванням пікселів,
в – помилково вилучений ЦВЗ

Як видно з подібності рис. 1.6,а і рис. 1.6,в матриці U_{w1} та V_{w1}, наявні у детектора містять надто суттєву інформацію, що неминуче призводить до помилки хибного спрацьовування.

Зі всіх існуючих наразі алгоритмів для більш детального дослідження було обрано алгоритм Fami [29]. Алгоритм ґрунтується на використанні ДПА. Відмінною особливістю алгоритму є зменшення обсягу вбудованої інформації ЦВЗ з допомогою обнуління частотних коефіцієнтів дискретного косинусного перетворення ЦВЗ. Вибір блоків, що модифікуються, заснований на аналізі

рівня ентропії зображення. Для вилучення ЦВЗ потрібно початкове зображення, що є недоліком. З іншого боку несліпий підхід до маркування цифрових зображень здатний збільшити стійкість вбудованого ЦВЗ до шкідливих впливів. Алгоритм Fami забезпечує відмінну стійкість до компресії зображення середнього рівня. З аналізу публікації [29] скритність ЦВЗ перебуває в достатньому рівні.

1.3 Методика дослідження стійкості вбудованого ЦВЗ

1.3.1 Складові методики аналізу стійкості

Виходячи з аналізу ряду робіт [19-29] для перевірки стійкості підходів та алгоритмів цифрового маркування до атак різного типу, зазвичай використовують методику, загальний алгоритм якої представлений на рис. 1.7. Перед його використанням необхідно визначити ряд параметрів (що будуть розглянуті у наступних підрозділах), які прямо чи опосередковано впливають на результати тестування.

Методику можна розділити на три основні етапи: використання ЦВЗ, атака на стегоконтейнер, вилучення водяного знаку. Після етапів маркування зображення визначається ступінь спотворення захищеного зображення шляхом порівняння з оригіналом із використанням певних метрик. Якщо досягнуто максимально-можливу якість стегоконтейнера, він піддається впливу низці атак. Інакше коригуються параметри вбудовування. Аналогічна процедура здійснюється і над вилученим ЦВЗ. Висновок про стійкість алгоритму ґрунтується на якості видобутого водяного знаку. Непомітність ЦВЗ визначається мірою видимості спотворень зображення-оригіналу.

Розглянемо докладніше основні етапи роботи методики дослідження стійкості вбудованого ЦВЗ [19-29].

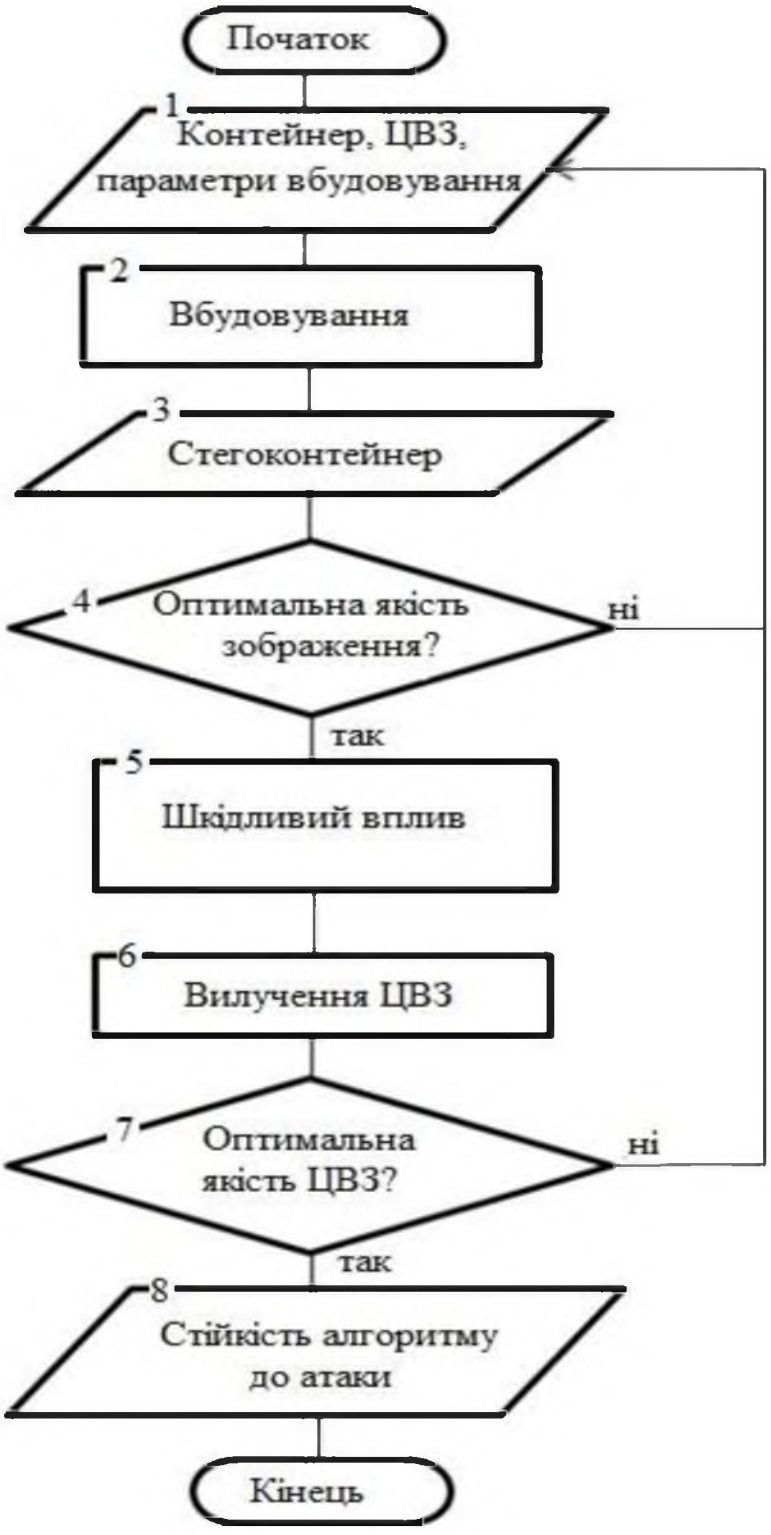


Рисунок 1.7 – Загальна схема алгоритму перевірки стійкості алгоритмів цифрового маркування до шкідливих впливів

1.3.1.1. Вибір контейнера та ЦВЗ.

Тестування алгоритму починається з вибору типу контейнера (у разі зображення) і ЦВЗ, куди він спочатку був орієнтований.

Існує кілька типів зображень, наприклад [30]:

• монохроматичне – найпростіший тип зображення, представлений кольорами двох типів: білим та чорним;

• напівтонове – представлене градаціями сірого кольору;

• кольорове – кожен піксель якого представлений трьома параметрами (наприклад, колірні моделі RGB, HLS тощо);

• безперервно-тонові (природні) – кольори або півтони сусідніх пікселів яких відрізняються один від одного на непомітну для людського ока величину;

• дискретно-тонові (синтетичні) – створені із використанням засобів обчислювальної техніки, характерною особливістю яких є відсутність плям і шумів, властивих природному зображенню;

• зображення типу «мультфільм» – що складаються з великих областей одного кольору або тону.

Як видно з наведеного вище опису, кожен тип зображення характеризується своїми властивостями, що необхідно враховувати при розробці та тестуванні стегоалгоритму. Так показники непомітності ЦВЗ, отримані при використанні монохроматичного зображення як контейнера можуть разюче відрізнятися від показників, отриманих у разі використання в якості контейнера кольорового зображення. Крім того варто враховувати, що процес впровадження ЦВЗ у кольорове зображення дещо відрізняється від маркування напівтонового зображення за рахунок складових колірних моделей і, як правило, включає ряд операцій, пов'язаних з перетворенням контейнера, що передують впровадженню ЦВЗ.

ЦВЗ у свою чергу можуть бути представлені:

• бітовою послідовністю;

• послідовністю символів;

• зображення.

Використання зображення як ЦВЗ зручно у зв'язку з включенням у процес розпізнавання поруч із декодером ЗСЛ. При допустимому рівні спотворень ЗСЛ зможе розпізнати вилучений ЦВЗ.

У цій роботі як контейнер вибрано природне напівтонове 8-бітне зображення – одне з найбільш простих і оптимальних у сучасних дослідженнях. Для об'єктивності результатів дослідження в якості контейнерів можуть бути використані декілька зображень, які відрізняються одне від одного за такими показниками, як гладкий фон, наявність рівних висококонтрастних областей і складних текстур. Як ЦВЗ вибрано монохроматичне чорне зображення, оскільки зміни у водяному знаку даного типу легше помітити у порівнянні з іншими типами зображення.

1.3.1.2. Параметри вбудовування.

Виходячи з обраної методики та заданого вище типу алгоритмів цифрового маркування, визначимо основні параметри, які підлягатимуть регулюванню при визначенні максимального рівня непомітності ЦВЗ та межі стійкості стегоалгоритму.

У адитивних алгоритмів, що використовують для вилучення водяного знаку зображення-оригінал, існує декілька формул злиття ЦВЗ із контейнером. Відповідно до [1], одна з найбільш поширених описується наступним чином:

$$c_i' = c_i \times (1 + \alpha \times w_i), \quad (1.5)$$

де c_i' – модифікований піксель контейнера (в даному випадку спектральний коефіцієнт); c_i – початковий піксель контейнера (початковий спектральний коефіцієнт); w_i – вбудований елемент водяного знаку (спектральний коефіцієнт); α – коефіцієнт посилення.

Крім формули (1.5) велике поширення також набула формула (1.6), що застосовується в алгоритмі [31]:

$$c_i' = c_i + \alpha \times w_i. \quad (1.6)$$

Вилучення ЦВЗ згідно з формулою (1.6) здійснюється відповідно до виразу:

$$w_i = (c_i' - c_i)/\alpha. \quad (1.7)$$

Виходячи з формул (1.5)-(1.7), одними з головних параметрів, які треба враховувати під час перевірки стійкості алгоритму цифрового маркування є:

• модифіковані спектральні коефіцієнти стегоконтейнера;

• коефіцієнт посилення – визначальний рівень зміни спектральних коефіцієнтів.

Коефіцієнт посилення може бути постійною величиною, або задаватися індивідуально залежно від властивостей кожного обраного блоку контейнера, тобто адаптивним. Вибір великого коефіцієнта посилення збільшує стійкість ЦВЗ, проте може сильно погіршити якість зображення, що захищається через занадто високий рівень зміни його спектральних коефіцієнтів. І навпаки – надмірно малий коефіцієнт робить ЦВЗ вкрай уразливим до шкідливих впливів.

Багато алгоритмів цифрового маркування задля досягнення непомітності ЦВЗ використовують ентропійне маскування – чим вище інформативність блоку, тим більше інформації можна у нього вбудувати. Тому не менш важливим параметром є поріг ентропії, який використовується в деяких алгоритмах для вибору блоків контейнера, що модифікуються.

Грамотний вибір спектральних коефіцієнтів дуже важливий задля досягнення стійкості ЦВЗ. Їх оптимальний вибір має бути теоретично обґрунтований. Тому для оптимальної вибірки частотних коефіцієнтів необхідно провести дослідження впливу стиску на ЦВЗ, вбудоване за допомогою перетворення Адамара.

Для досягнення найкращих показників непомітності у разі використання ентропійного маскування необхідне визначення залежності між рівнем ентропії конкретного блоку контейнера та допустимим обсягом вбудованої інформації, що не призводить до видимих спотворень.

1.3.1.3. Вибір метрик визначення якості стегоконтейнера та ЦВЗ.

Для правильної інтерпретації результатів моделювання, пов'язаних з визначенням ступеня невидимості та стійкості ЦВЗ, необхідний грамотний підхід до вибору метрик, що визначають ступінь якості маркованого зображення та видобутого з нього водяного знаку. Існує велика різноманітність показників візуального спотворення зображень, які поділяються на [1-3, 5-7]:

• різницеві – засновані на відмінності між контейнером (початковий сигнал) та стегоконтейнером (спотворений сигнал);

• кореляційні – засновані на кореляції між початковим зображенням та стегоконтейнером;

• інші показники, які не входять за своїми характеристиками у дві вище перелічені категорії.

Наразі немає абсолютно-об'єктивної міри спотворення зображення. У сучасних дослідженнях найбільш поширеним показником якості захищеного зображення використовується пікове відношення сигналу до шуму (PSNR – Peak Signal to Noise Ratio):

$$PSNR = 10\log_{10}\frac{255^2 * M * N}{\sum_{x,y}(f(x,y)-\hat{f}(x,y))^2}, \quad (1.8)$$

де $f(x, y)$ та $\hat{f}(x,y)$ – початкове та захищене зображення; x, y – координати пікселів; M та N – висота та ширина зображення.

Вважається, що зміни зовнішнього вигляду початкового зображення непомітні, якщо PSNR не нижче 43 дБ. Однак при оцінюванні зовнішнього вигляду стегоконтейнера з використанням різницевих показників обов'язково необхідно враховувати зорову систему людини. Навіть якщо показник PSNR перевищує 43 дБ, є можливість, що людському оку можуть бути помітні спотворення зображення. Цей факт є основним недоліком різницевих показників і пов'язаний з відсутністю їхньої кореляції із ЗСЛ.

Після того, як досягнуті оптимальні параметри впровадження ЦВЗ, здійснюється перевірка алгоритму цифрового маркування на стійкість до атак різного типу, серед яких найбільш поширеними є: компресія зображення, вплив шумів різного типу та фільтрація зображення, що призводять до сильного спотворення або повного знищення водяного знаку.

Як міру якості одержаного ЦВЗ найбільшого поширення набули кореляційні показники якості, наприклад коефіцієнт кореляції Пірсона:

$$k = \frac{\sum_c \sum_r (A(c,r) - A_m) * (B(c,r) - B_m)}{\sqrt{\sum_c \sum_r \left((A(c,r) - A_m)^2\right) * \left(\sum_c \sum_r (B(c,r) - B_m)^2\right)}}, \quad (1.9)$$

де c, r – координати пікселя зображення; A(c, r), B(c, r) – початковий та вилучений ЦВЗ; A_m, B_m – середнє арифметичне величин яскравості пікселів початкового та вилученого ЦВЗ, відповідно.

Значення коефіцієнта кореляції визначено в діапазоні від -1 до 1. Вилучений ЦВЗ вважають стійким до певної атаки, якщо його коефіцієнт кореляції не нижче 0.5. У разі повної ідентичності видобутого ЦВЗ даний показник набуває значення, що дорівнює 1.

1.4 Висновок. Постановка задачі

Проведено класифікацію алгоритмів цифрового маркування нерухомих зображень, з яких частотні алгоритми цифрового маркування є найбільш підходящими для протидії атак компресії.

Найбільш перспективним перетворенням є дискретне перетворення Адамара, використовуючи яке ЦВЗ здатний протистояти незалежній від платформи компресії (JPEG або JPEG2000).

При використанні сингулярного розкладання в алгоритмах цифрового маркування необхідна ретельна перевірка на наявність помилкового спрацьовування стеганодетектора.

Обґрунтована методика тестування алгоритмів цифрового маркування: вибрано типи контейнера та ЦВЗ, визначено вхідні параметри та метрики аналізу якості.

Подальші дослідження мають бути спрямовані на:

• проведення аналізу впливу JPEG стиснення на частотні коефіцієнти обраного ортогонального перетворення;

• дослідження та удосконалення алгоритмів цифрового маркування, які забезпечують стійкість ЦВЗ до різноманітних атак.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Втрата інформації при JPEG стисненні

Загальна схема JPEG стиснення представлена рис. 2.1 [35]. Докладно розглянемо ті етапи компресії, у яких відбувається основна втрата інформації зображення.

Рисунок 2.1 – Основні етапи процедури стиснення за стандартом JPEG

Як видно з рис. 2.1, основним операціям перетворення зображення передує його попередня обробка – перехід з RGB схеми в YCbCr (етап 1) з її подальшою дискретизацією (етап 2). Далі зображення розбивається на однакові блоки пікселів розміром 8×8, кожен із яких піддається ДКП (етап 3), що здійснюється за формулою 6.

$$ДКП(i,j) = C(i) * C(j) * \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) * cos\left[\frac{(2x+1)i\pi}{2N}\right] * cos\left[\frac{(2y+1)j\pi}{2N}\right], \quad (2.1)$$

де $C(i), C(j) = \begin{cases} \sqrt{\frac{1}{N}} \text{ при } i,j = 0 \\ \sqrt{\frac{2}{N}} \text{ при } i,j = 1,2,\dots,N-1 \end{cases}$, f(x, y) – піксель зображення.

Внаслідок застосування ДКП отримуємо матрицю коефіцієнтів ДКП. На цьому етапі відбувається перерозподіл енергії кожного блоку зображення, що супроводжується незначною втратою інформації зображення, зумовленою похибкою обчислення ДКП. Низькочастотні складові кожного блоку знаходяться в області лівого верхнього кута матриці коефіцієнтів. У нижньому правому куті знаходяться високочастотні складові. Коефіцієнт, розташований у верхньому лівому куті, називається DC-коефіцієнтом. Він містить переважну частину енергії блоку. Інші коефіцієнти називаються AC-коефіцієнтами. Чим ближче AC-компонент до правого нижнього кута таблиці коефіцієнтів, тим вище його частота. На рис. 2.2 представлені приклади перерозподілу енергії зображення за допомогою ДКП для гладкої текстури, та складної – рис. 2.3.

171	172	174	172	172	173	174	176
172	169	174	176	175	178	177	173
174	171	178	174	175	170	176	174
173	171	171	174	174	174	176	174
170	172	171	172	171	172	173	172
172	176	171	171	171	175	175	175
174	173	172	175	175	175	175	160
174	173	173	175	175	171	174	174

а

1385,50	-3,39	-2,76	1,68	-1,75	4,19	-2,10	1,57
2,41	-5,28	1,03	-3,84	0,95	0,55	3,97	1,55
1,78	1,45	-2,16	0,33	0,34	0,55	0,54	0,65
-3,67	-0,91	2,24	1,19	-3,96	-3,00	-0,13	-4,08
-2,25	-2,16	3,25	-3,26	3,00	-2,42	0,01	-0,99
-0,83	3,50	-1,56	2,74	-1,22	1,29	-1,59	1,26
1,70	-0,75	6,54	-6,40	1,48	-3,64	0,66	1,53
-3,19	4,29	-2,39	-1,22	-0,76	1,24	-0,48	2,80

б

Рисунок 2.2 – Перерозподіл енергії: а – гладка текстура; б – коефіцієнти ДКП гладкої текстури

208	244	108	173	71	112	181	245
231	246	234	193	12	97	192	87
32	40	202	189	25	195	70	149
233	248	245	100	210	203	173	57
161	244	167	167	177	48	167	192
25	124	9	44	81	125	41	65
71	204	217	180	242	114	30	129
139	36	238	8	9	165	127	178

а

1116,13	102,47	44,85	-99,15	-95,38	-24,60	40,01	-26,14
135,21	58,72	79,59	-20,98	-9,77	108,64	-71,45	-85,82
-17,91	-31,36	99,05	-58,11	3,41	53,09	64,48	-30,85
-20,26	10,15	43,98	21,87	90,44	-104,04	-189,06	-45,88
142,38	1,78	135,95	34,85	0,87	5,43	-16,40	80,74
60,05	0,43	-112,21	42,68	29,49	-102,01	7,72	4,15
-210,82	-168,90	23,73	21,92	0,07	15,28	97,45	-79,94
36,65	-64,61	-47,04	-135,14	94,39	-15,52	0,06	-26,08

б

Рисунок 2.3 – Перерозподіл енергії: а – складна текстура; б – коефіцієнти ДКП складної текстури

Як видно з рис. 2.2-2.3, для складної текстури характерна більша концентрація енергії в АС-коефіцієнтах, ніж АС-коефіцієнти гладкої текстури.

Після перерозподілу енергії здійснюється квантування коефіцієнтів ДКП. На цьому етапі відбувається основна втрата інформації зображення. Операція квантування полягає у розподілі кожного елемента матриці ДКП на відповідний елемент матриці квантування з подальшим округленням приватного до найближчого цілого.

Стандарт JPEG дозволяє користувачеві задавати власну таблицю квантування. Однак найбільшого поширення набули таблиці, наведені в стандарті JPEG. На рис. 2.4-2.5 відображено дані таблиці квантування для яскравості та колірної складової, відповідно.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Рисунок 2.4 – Таблиця квантування яскравості

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Рисунок 2.5 – Таблиця квантування колірної складової

З значень таблиць квантування (рис. 2.4-2.5) видно, що найбільшій зміні піддаються високочастотні коефіцієнти, як менш значущі.

Для регулювання ступеня стиснення в алгоритмі JPEG існує коефіцієнт якості Q, який знаходиться в діапазоні від 0 до 100. Чим менший коефіцієнт якості, тим вище рівень згортання. Таблиці, представлені на рис. 2.4 і 2.5, відповідають Q=50. Щоб визначити коефіцієнт квантування для інших значень Q, визначається коефіцієнт масштабування S [32]:

$$S = \begin{cases} \frac{5000}{Q}, \text{если } Q < 50 \\ 200 - 2 * Q, \text{если } Q \geq 50 \end{cases} \quad (2.2)$$

Нова таблиця квантування будується згідно формули:

$$T_s[i,j] = \left\lfloor \frac{S*T_b[i,j]+50}{100} \right\rfloor, \quad (2.3)$$

де T – початкова таблиця квантування для Q=50; T_S – масштабована таблиця квантування; (i, j) – координати коефіцієнта у таблиці.

Кожен одержаний за формулою (2.2) елемент таблиці округляється у бік меншого цілого числа. Однак якщо отриманий елемент менше 1, йому присвоюється значення 1. Якщо отриманий елемент таблиці більше 255, то йому присвоюється значення 255. При Q=100 всі елементи таблиці квантування приймають значення, рівне 1, при Q=0 – значення, рівні 255. Отже, можливі значення елементів даної таблиці квантування укладені в інтервалі від 1 до 255.

На наступних етапах (кроки 5-7, рис. 2.1) немає необоротної втрати інформації. Після квантування таблиця отриманих коефіцієнтів кожного блоку зображення вишиковується у вектор за допомогою зигзаг-сканування, починаючи з DC-коефіцієнта у бік нижнього правого кута таблиці. В результаті утворюється набір векторів-рядків, у кожному з яких утворюється більше кількість нульових послідовностей, що забезпечує подальшу ефективність стиснення без втрат на кроках 6 (стиснення RLE) і 7 (стиснення Хафмана).

Процес відновлення зображення аналогічний до процесу стиснення, але всі кроки виконуються у зворотному порядку (рис. 2.1). Однак, замість процедури квантування коефіцієнтів ДКП здійснюється процедура їх деквантування, в результаті якої кожен квантований коефіцієнт множиться на таблицю квантування, що використовується при стисненні. Для відновлення значень яскравості використовується зворотне ДКП, яке здійснюється наступним чином:

$$f(x,y) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(i) * C(j) * \text{ДКП}(x,y) * cos\left[\frac{(2x+1)i\pi}{2N}\right] * cos\left[\frac{(2y+1)j\pi}{2N}\right], \quad (2.4)$$

$$C(i), C(j) = \begin{cases} \sqrt{\frac{1}{N}} \text{ при } i,j = 0 \\ \sqrt{\frac{2}{N}} \text{ при } i,j = 1,2,\dots,N-1 \end{cases}$$

де

На рис. 2.6-2.7 наведено приклади коефіцієнтів ДКП гладкої та складної текстур, що пройшли процедури квантування, а потім деквантування з використанням таблиці квантування для Q=50.

1385,50	-3,39	-2,76	1,68	-1,75	4,19	-2,10	1,57
2,41	-5,28	1,03	-3,84	0,95	0,55	3,97	1,55
1,78	1,45	-2,16	0,33	0,34	0,55	0,54	0,65
-3,67	-0,91	2,24	1,19	-3,96	-3,00	-0,13	-4,08
-2,25	-2,16	3,25	-3,26	3,00	-2,42	0,01	-0,99
-0,83	3,50	-1,56	2,74	-1,22	1,29	-1,59	1,26
1,70	-0,75	6,54	-6,40	1,48	-3,64	0,66	1,53
-3,19	4,29	-2,39	-1,22	-0,76	1,24	-0,48	2,80

а

1392	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

б

Рисунок 2.6 – Квантування коефіцієнтів ДКП гладкої текстури: а – коефіцієнти ДКП; б – відновлені коефіцієнти ДКП

Як видно з прикладів (рис. 2.6-2.7), всі АС-коефіцієнти гладкої текстури були знищені у процесі квантування. У той же час, за рахунок більшої концентрації енергії основна частина АС-коефіцієнтів складної текстури збереглась. Таким чином, при стисненні JPEG найбільша втрата інформації відбувається при квантуванні коефіцієнтів ДКП, при якому більша кількість інформації зберігається в складних блоках текстур. Отже, складні текстури найбільш підходять для вбудовування ЦВЗ.

1116,13	102,47	44,85	-99,15	-95,38	-24,60	40,01	-26,14
135,21	58,72	79,59	-20,98	-9,77	108,64	-71,45	-85,82
-17,91	-31,36	99,05	-58,11	3,41	53,09	64,48	-30,85
-20,26	10,15	43,98	21,87	90,44	-104,04	-189,06	-45,88
142,38	1,78	135,95	34,85	0,87	5,43	-16,40	80,74
60,05	0,43	-112,21	42,68	29,49	-102,01	7,72	4,15
-210,82	-168,90	23,73	21,92	0,07	15,28	97,45	-79,94
36,65	-64,61	-47,04	-135,14	94,39	-15,52	0,06	-26,08

а

1120	99	40	-96	-96	-40	51	0
132	60	84	-19	0	116	-60	-110
-14	-26	96	-48	0	57	69	-56
-14	17	44	29	102	-87	-160	-62
144	0	148	56	0	0	0	77
72	0	-110	64	0	-104	0	0
-196	-192	0	0	0	0	120	-101
72	-92	0	-98	112	0	0	0

б

Рисунок 2.7 – Квантування коефіцієнтів ДКП складної текстури:
а – коефіцієнти ДКП; б – відновлені коефіцієнти ДКП

2.2 Вплив JPEG стиснення на коефіцієнти перетворення Адамара

Оскільки для дослідження було обрано алгоритми цифрового маркування, що ґрунтуються на використанні ДПА, необхідно визначити взаємозв'язок між коефіцієнтами даного перетворення та ДКП, оскільки саме коефіцієнти ДКП піддаються квантуванню у процесі стиснення JPEG.

2.2.1 Перетворення Адамара

ДПА належить до класу ортогональних перетворень у діадних базисах, обчислювальна складність якого менша у порівнянні з ДКП та ДВП. Ядром цього перетворення є матриця Адамара. Елементи даної матриці приймають

значення 1 та -1. Матриця Адамара описує перетворення, пов'язане з розкладанням функцій сімейства прямокутних базисних функцій.

Як правило, як ядро ДПА використовується матриця порядку $N=2^n$, де n – ціле число. Матриця ядра ДПА має властивість симетричності, тобто

$$A_N = A_N^T \tag{2.5}$$

Ядро ДПА порядку $N=2^n$, де n – ціле позитивне число, що формуються за допомогою операції кронекерівського множення матриць:

$$A_{2N} = A_N \otimes A_2 = \begin{bmatrix} A_N & A_N \\ A_N & -A_N \end{bmatrix}, \tag{2.6}$$

де $A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ – матриця Адамара найменшого порядку.

В алгоритмах цифрового маркування нерухомих зображень, зазвичай, використовують ядро ДПА порядку N=8, оскільки при компресії JPEG зображення також розбивається на блоки розміром 8×8. Дане ядро представлено рис. 2.8.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Рисунок 2.8 – Матриця Адамара розміром 8×8

Число змін знаку рядків матриці аналогічно частотній концепції перетворення Фур'є. Так само, як і у ДКП основна енергія зображення під час використання ДПА зосереджена в DC-коефіцієнті (верхній лівий кут таблиці коефіцієнтів), інші коефіцієнти – AC. При цьому умовно вважається, що частота коефіцієнтів тим більша, чим більше число змін знаків у відповідному рядку / стовпці матриці ядра ДПА.

Двовимірне перетворення Адамара визначається наступним чином:

$$f_{KL} = \frac{1}{N}\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} x_{mn}(-1)^{km+nl}, \tag{2.7}$$

де m, n – індекси пікселя початкового зображення; k, l – індекси коефіцієнтів ДПА.

Зворотне перетворення Адамара еквівалентне прямому перетворенню внаслідок симетричності ядра перетворення Адамара.

Ядро ДПА має властивість роздільності ядра перетворення по змінним підсумовування, отже, для зменшення обчислювальної складності пряме і зворотне ДПА може бути обчислено рядково-стовпцевим способом, при якому одномірні ДПА послідовно застосовуються до рядків матриці початкових даних, а потім до стовпців отриманої матриці проміжних даних:

$$F_N = \frac{1}{N} A_N [X_N A_N], \tag{2.8}$$

де X_N – початкове зображення (у разі прямого ДПА) або матриця частотних коефіцієнтів (у разі зворотного ДПА), F_N – матриця коефіцієнтів ДПА зображення (у разі прямого ДПА) або матриця пікселів зображення (у разі зворотного ДПА), N – розмір матриці, що перетворюється. Рядково-стовпцевий метод дозволяє скоротити обсяг обчислень з N^4 до $2N^3$ базових операцій.

Для більшого зменшення обчислювальної складності можна використовувати алгоритм швидкого перетворення Адамара, який дозволить скоротити кількість базових операцій з N^2 до $(N \times \log_2 N)/2$ під час кожного одновимірного перетворення.

2.2.2 Взаємозв'язок коефіцієнтів ДПА та ДКП

Для визначення взаємозв'язку між коефіцієнтами ДПА та ДКП було проведено моделювання в середовищі Matlab/Simulink, послідовність дій якого така:

- генерація напівтонової текстури розміром 8×8;

• обчислення коефіцієнтів ДПА та ДКП отриманої матриці пікселів;

• почергова зміна кожного коефіцієнта одержаної матриці ДПА;

• обчислення зворотного ДПА з одержанням видозміненої текстури;

• обчислення двовимірного ДКП видозміненої текстури з метою визначення змін початкових коефіцієнтів цього перетворення.

Аналогічні операції проводилися при зміні коефіцієнтів ДКП. В результаті моделювання було виявлено 5 груп взаємопов'язаних коефіцієнтів ДПА та ДКП. Зміна будь-якого коефіцієнта групи одного перетворення призводить до зміни всіх коефіцієнтів відповідного набору тієї ж групи іншого перетворення. Відповідність між коефіцієнтами ДКП $d_{y,x}$ та ДПА $a_{y,x}$ представлено в табл. 2.1.

У табл. 2.1 представлено положення взаємозалежних коефіцієнтів ДКП та ДПА, зміна яких була суттєвою. Зміни коефіцієнтів порядку 10-12 і менше не враховувалисm через їх незначність у контексті завдання цифрового маркування. Найбільш примітною є перша група, в якій величина коефіцієнтів двох перетворень практично ідентична. Отже, якщо алгоритмах цифрового маркування змінювати коефіцієнти першої групи, то стійкість під час використання ДПА має практично повністю відповідати стійкості того ж алгоритму, але заснованого на ДКП. Також, подібні алгоритми суттєво виграватимуть у зменшенні обчислювальної складності.

Для інших груп зміна одного коефіцієнта пропорційно до сумарної зміни відповідної групи коефіцієнтів іншого перетворення (див. табл. 2.1). При цьому найбільшій зміні підлягає коефіцієнт, близький до діапазону частот модифікованого частотного компонента іншого перетворення. Пари таких коефіцієнтів мають дуже схожі коливання по всьому діапазоні значень параметра якості JPEG.

Приклад такої подібності (порівняння коливань подібних частотних складових ДПА та ДКП для будь-якого показника якості JPEG) представлено на рис. 2.9 для $a_{1,5}$ та $d_{1,2}$.

Таблиця 2.1 – Взаємозв'язок коефіцієнтів ДКП та ДПА

Групи коефіцієнтів	$d_{v.x}$	$a_{v.x}$
1-коефіцієнтна	1,1	1,1
	1,5	1,4
	5,1	4,1
	5,5	4,4
2-коефіцієнтна	1,3 1,7	1,6 1,7
	3,1 7,1	6,1 7,1
	3,5 7,5	6,4 7,4
	5,3 5,7	4,6 4,7
4-коефіцієнтна	1,2 1,4 1,6 1,8	1,2 1,3 1,5 1,8
	5,2 5,4 5,6 5,8	4,2 4,3 4,5 4,8
	2,1 4,1 6,1 8,1	2,1 3,1 5,1 8,1
	2,5 4,5 6,5 8,5	2,4 3,4 5,4 8,4
	3,3 3,7 7,3 7,7	6,6 6,7 7,6 7,7
8-коефіцієнтна	2,3 2,7 4,3 4,7 6,3 6,7 8,3 8,7	2,6 2,7 3,6 3,7 5,6 5,7 8,6 8,7
	3,2 3,4 3,6 3,8 7,2 7,4 7,6 7,8	6,2 6,3 6,5 6,8 7,2 7,3 7,5 7,8
16-коефіцієнтна	2,2 2,4 2,6 2,8 4,2 4,4 4,6 4,8 6,2 6,4 6,6 6,8 8,2 8,4 8,6 8,8	2,2 2,3 2,5 2,8 3,2 3,3 3,5 3,8 5,2 5,3 5,5 5,8 8,2 8,3 8,5 8,8

Виходячи з того, що в процесі JPEG стиснення найменшому квантуванню піддаються низькочастотні компоненти ДКП і на основі аналізу взаємозалежності компонентів ДПА та ДКП були обрані теоретично найбільш стійкі до компресії коефіцієнти дискретного перетворення Адамара. Їх розташування в матриці представлено на рис. 2.10,а.

Рисунок 2.9 – Порівняння коливань подібних частотних складових ДПА та ДКП для будь-якого показника якості JPEG

Порядок обраних компонентів ДПА a_i у бік збільшення частотності: 1,1; 1,5; 5,1; 1,7; 5,5; 7,1; 3,1; 7,5; 5,7; 1,3; 1,4; 5,3; 7,7; 3,5; 4.1. Відповідні коефіцієнти ДКП d_i розташовані в порядку зигзаг-сканування (рисунок 2.10,б): 1,1; 1,2; 2,1; 3,1; 2,2; 1,3; 1,4; 2,3; 3,2; 4,1; 5,1; 4,2; 3,3; 2,4; 1,5.

1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8
2,1	2,2	2,3	2,4	2,5	2,6	2,7	2,8
3,1	3,2	3,3	3,4	3,5	3,6	3,7	3,8
4,1	4,2	4,3	4,4	4,5	4,6	4,7	4,8
5,1	5,2	5,3	5,4	5,5	5,6	5,7	5,8
6,1	6,2	6,3	6,4	6,5	6,6	6,7	6,8
7,1	7,2	7,3	7,4	7,5	7,6	7,7	7,8
8,1	8,2	8,3	8,4	8,5	8,6	8,7	8,8

а

1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8
2,1	2,2	2,3	2,4	2,5	2,6	2,7	2,8
3,1	3,2	3,3	3,4	3,5	3,6	3,7	3,8
4,1	4,2	4,3	4,4	4,5	4,6	4,7	4,8
5,1	5,2	5,3	5,4	5,5	5,6	5,7	5,8
6,1	6,2	6,3	6,4	6,5	6,6	6,7	6,8
7,1	7,2	7,3	7,4	7,5	7,6	7,7	7,8
8,1	8,2	8,3	8,4	8,5	8,6	8,7	8,8

б

Рисунок 2.10 – Низькочастотні коефіцієнти ДПА (а), що відповідають низькочастотним компонентам ДКП (б)

2.3 Дослідження алгоритму Fami

Для дослідження ефективності перетворення Адамара в області цифрового маркування нерухомих зображень було обрано відомий алгоритм Fami [29], що поєднує в собі відносну простоту реалізації та стійкість впровадженого ЦВЗ до стиску JPEG. Алгоритм не є сліпим, тобто для отримання вбудованої інформації необхідний початковий контейнер. Подібний підхід спрощує завдання протидії деяким шкідливим впливам, наприклад, компресії або зміни розміру. Алгоритм Fami призначений для напівтонових зображень.

Відмінною особливістю алгоритму Fami є попередня обробка ЦВЗ, що імітує процес стиску JPEG. Основна мета операції – суттєво скоротити обсяг вбудованої інформації без значного зменшення зовнішнього вигляду ЦВЗ. Водяний знак розбивається на блоки розміром K×K, до кожного з яких застосовується ДКП. Кожна отримана матриця коефіцієнтів вибудовується у вектор-рядок з використанням алгоритму зигзаг-сканування. У кожного рядка зберігаються тільки L коефіцієнтів, що йдуть поспіль, починаючи з першого. Далі усі рядки поєднуються в єдиний рядок, елементи якого й будуть вбудовані в контейнер.

Після операції попередньої обробки контейнер розбивається на блоки розміром M×M. Серед одержаних блоків вибираються найінформативніші. Як правило, алгоритми, подібні до Fami, для оцінки складності текстури використовують такий параметр, як ентропія зображення, яка найчастіше визначається за формулою Шеннона:

$$E = -\sum_{i=1}^{n} p_i log_2(p)_i \,, \tag{2.9}$$

де p_i – ймовірність виникнення пікселя з відповідною яскравістю в блоці p. Ймовірність p знаходиться в інтервалі [0; 1]. Сума ймовірностей всіх типів яскравостей блоку дорівнює 1. Чим вище значення ентропії масиву пікселів, тим складніша текстура. Ентропія абсолютно гладкої текстури (кожен елемент якої має однакові значення яскравості) дорівнює нулю.

В алгоритмі Fami спочатку оцінюється ентропія навколо кожного пікселя обраного блоку, потім обчислюється середнє значення. Блоки, чия ентропія перевищує заданий поріг, піддаються ДПА для подальшого вбудовування ЦВЗ. Вбудовування здійснюється згідно (1.6). Коефіцієнт посилення вибирається заздалегідь і залишається постійним протягом всього процесу вбудовування. Після вбудовування виконується зворотне ДПА. Модифіковані та незмінені блоки об'єднуються.

Процес отримання водяного знаку здійснюється аналогічно, але усі операції виконуються в зворотному порядку. Початкове зображення-контейнер необхідне для визначення місцезнаходження модифікованих блоків стегоконтейнера. Вилучення частотного коефіцієнта ЦВЗ здійснюється згідно (1.7). Сформований вектор рядок розбивається на однакові блоки, довжина яких була визначена при вбудовуванні ЦВЗ. З кожного рядка формується матриця коефіцієнтів ДКП розміром K×K. Кожен блок піддається зворотному ДКП. Отримані матриці поєднуються, тим самим відновлюючи вбудований ЦВЗ.

Таким чином, алгоритм Fami має такі регульовані параметри:

• положення (y, x) модифікованих коефіцієнтів вбудовування в блоці;

• K, M – розміри блоків декомпозиції ЦВЗ та контейнера;

• коефіцієнт сили вбудовування прихованої інформації;

• L – кількість збережених коефіцієнтів кожного блоку K×K ЦВЗ;

• поріг ентропійного маскування E.

Дослідимо вплив даних параметрів на непомітність вбудовування ЦВЗ та її стійкість до різних атак визначення шляхів вдосконалення алгоритму.

2.3.1 Аналіз непомітності ЦВЗ, вбудованого алгоритмом Fami

З перерахованих вище параметрів вплив на непомітність вбудованого ЦВЗ має вибір положення коефіцієнтів, що модифікуються, поріг ентропії E і коефіцієнт сили вбудовування α.

Для визначення впливу даних параметрів на непомітність ЦВЗ було проведено моделювання в середовищі Matlab/Simulink. Як контейнер було вибрано стандартне зображення «Lena». Як параметри K, M, L і α обрані значення, які використовував автор алгоритму Fami, а саме: 8, 8, 15 і 35. Поріг ентропії підбирався таким чином, щоб задіяти для вбудовування якомога більше складних текстур. Після визначення максимально допустимого порога ентропії виконувалася оцінка коефіцієнта ДПА, що викликає найменші спотворення.

В результаті імітаційного моделювання було встановлено, що якщо в зображенні мало складних текстур, їх буде неможливо ефективно використовувати, тому що коефіцієнт α є константою, і, отже, вбудовування ЦВЗ в текстури з низьким рівнем ентропії вимагає малого коефіцієнта посилення α для непомітності. В іншому випадку будуть помітні артефакти впровадження. Теоретично, цей недолік повинен позначитися також і на робастності вбудованого водяного знаку, яка тим краща, чим більший коефіцієнт сили вбудовування.

При однаковому значенні параметра для блоків з високою ентропією найбільша непомітність досягалася при використанні низькочастотних коефіцієнтів для вбудовування (для $a_{1,5}$). Найкраща непомітність спостерігалася при використанні DC-коефіцієнта.

Однак варто враховувати, що використання DC-коефіцієнта теоретично може зробити ЦВЗ вкрай уразливим до атак стегоконтейнера, спрямованим на зміну яскравості пікселів. Зі збільшенням частотності коефіцієнта, що використовується для блоків з високою ентропією збільшувалася помітність спотворень (для $a_{2,2}$), що проявляється в утворенні областей з порогами малої площі, але більшої інтенсивності.

Було встановлено, що PSNR=43,2 дБ, що означає високий рівень непомітності спотворень, що вносяться в контейнер.

2.3.2 Аналіз стійкості алгоритму Fami до шкідливих впливів

Оцінка опірності алгоритму Fami компресії JPEG2000, шуму, фільтрації, масштабування, була зроблена з використанням параметрів, що забезпечують найбільшу стійкість до компресії JPEG. Крім перевірки стійкості, оцінці підлягала ефективність використання ДПА порівняно з ДКП та ДВП на основі даного алгоритму. Для цього головне перетворення алгоритму послідовно замінювалося на два останні з повторенням шкідливих впливів на стегоконтейнер.

Параметри алгоритму для моделювання: K=8, M=8, L=15, α=35. Як контейнер було вибрано стандартне зображення «Lena». Як ЦВЗ було використано монохромне чорно-біле зображення розміром 64×64. Як змінені коефіцієнти обрані такі, які найбільш близькі за низькочастотним діапазоном, а саме коефіцієнт ДПА kDHadT(1, 5), коефіцієнт ДКП kDCT(1, 2), коефіцієнт дискретного перетворення Хаара (ДПХ) kDHaarT(1, 4), коефіцієнт дворівневого ДПХ kDHaarT2(1, 2).

Насамперед алгоритм був перевірений на стійкість до стиснення JPEG. Після застосування ЦВЗ стегоконтейнер піддавався компресії з наступним вилученням ЦВЗ. Подібна операція повторювалася для всього діапазону коефіцієнта якості Q (від 100 до 0). Результати моделювання наведено рис. 2.11. Встановлено, що алгоритм Fami показує хорошу стійкість до стиску JPEG. ЦВЗ розпізнається включно до коефіцієнта якості Q=5. Однак, починаючи з Q=10, стійкість ЦВЗ починає різко знижуватися. Як і очікувалося, при використанні ДКП були досягнуті вищі результати стійкості, що пов'язано з використанням аналогічного перетворення в стисненні JPEG. Використання ДПХ показує найгірші результати, оскільки процес отримання частотних коефіцієнтів з їх допомогою відрізняється від ДКП і ДПА. Збільшення рівня вкладення коефіцієнтів ЦВЗ під час використання дворівневого ДПХ покращує показники стійкості, проте обчислювальна складність при цьому сильно зростає, що позначається на швидкості виконання алгоритму.

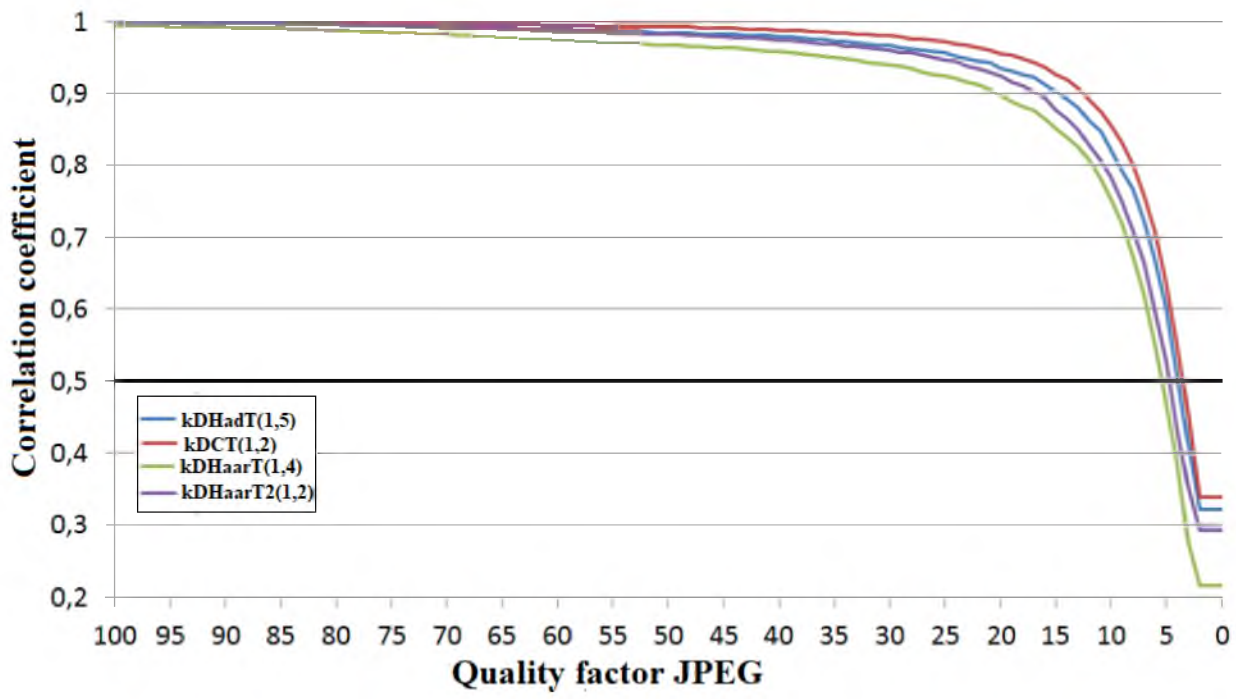


Рисунок 2.11 – Стійкість алгоритму Fami до стиснення JPEG

Результати стійкості алгоритму Fami проти стиснення JPEG2000 для рівнів стиснення до 56 разів включно представлені рис. 2.12.

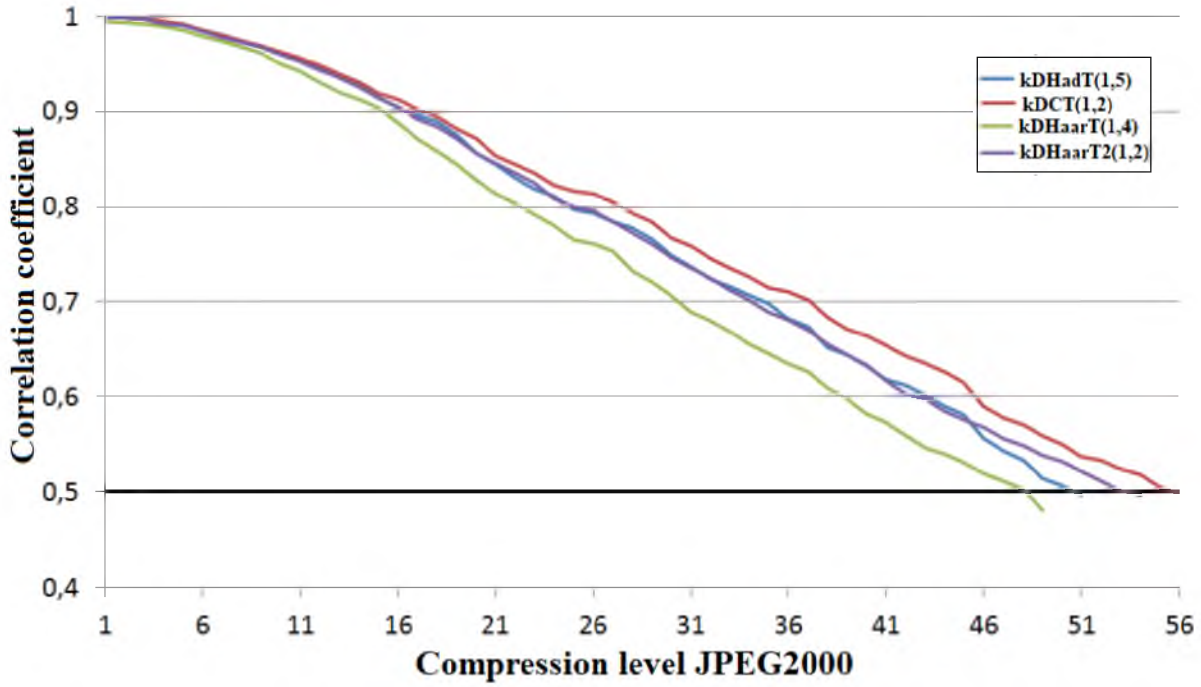


Рисунок 2.12 – Стійкість алгоритму Fami до стиснення JPEG2000

Встановлено, що найкращі показники стійкості до стиснення JPEG2000 забезпечує ДКП. При його використанні ЦВЗ зберігається у допустимій якості до 55-кратного стиснення, що є недостатнім, оскільки зображення за такого рівня компресії зберігає свої комерційні властивості. Використання ДПА забезпечує схожі показники. При цьому підході до вбудовування використання ДПХ першого та другого рівнів є неефективним через низькі показники першого та високу обчислювальну складності другого перетворень.

Іншим видом шкідливого впливу є зашумлення. Одними з найшкідливіших є гаусівський шум (адитивний шум) і шум «сіль і перець» (імпульсний шум). Стегоконтейнер був зашумлений при зміні дисперсії від 0,01 до 0,1, при якому рівень спотворень зображення досягає досить високого рівня. Результати наведено на рис. 2.13 та 2.14.

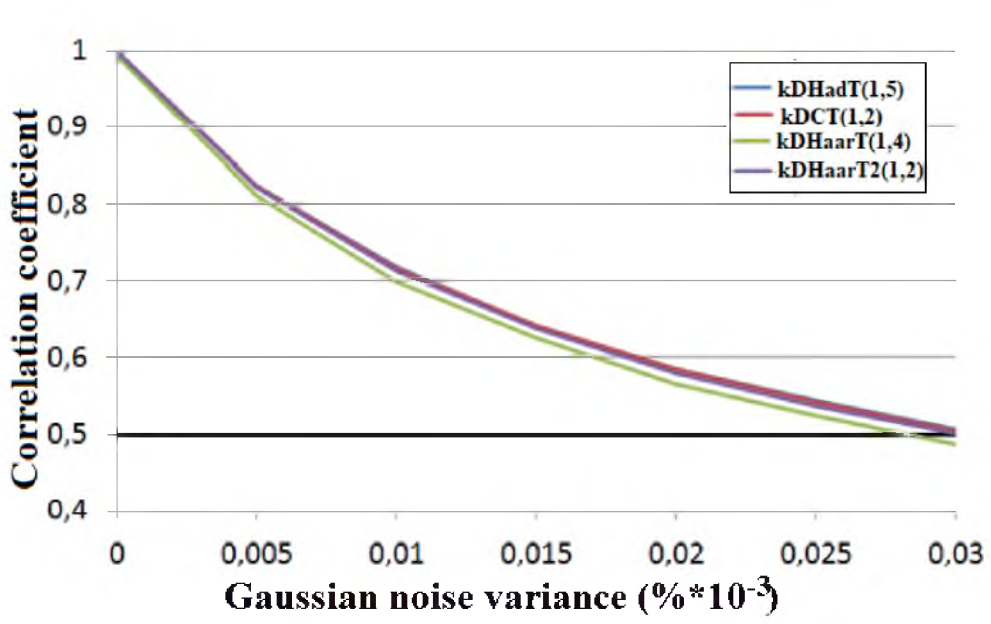


Рисунок 2.13 – Стійкість алгоритму Fami до шуму Гауса

Встановлено, що алгоритм Fami забезпечує стійкість ЦВЗ до шуму Гауса рівня дисперсії 0,03, що є достатнім (рис. 2.13). А стійкість ЦВЗ до шуму «сіль і перець» зберігається до дисперсії 0,085 (рис. 2.14). Вибір ДПА, ДКП, ДПХ при цьому підході до цифрового маркування не істотно впливає на стійкість ЦВЗ до зашумлення.

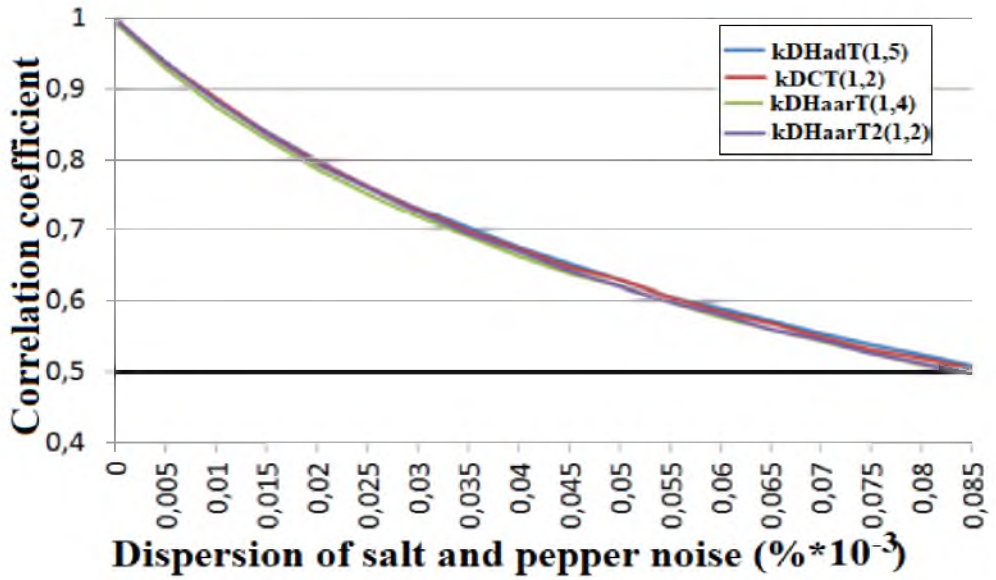


Рисунок 2.14 – Стійкість алгоритму Fami до шуму «сіль і перець»

Для усунення ЦВЗ зловмисники можуть активно використовувати фільтрацію зображення, оскільки вона здатна ефективно усувати спотворення, спричинені зашумленням. У ході моделювання було обрано фільтр Вінера розміром а×а, який ефективно усуває шум Гауса, і який застосовувався до стегоконтейнера. Вікно фільтрації послідовно збільшувалося від 2 до 16. Результати стійкості представлені на рис. 2.15.

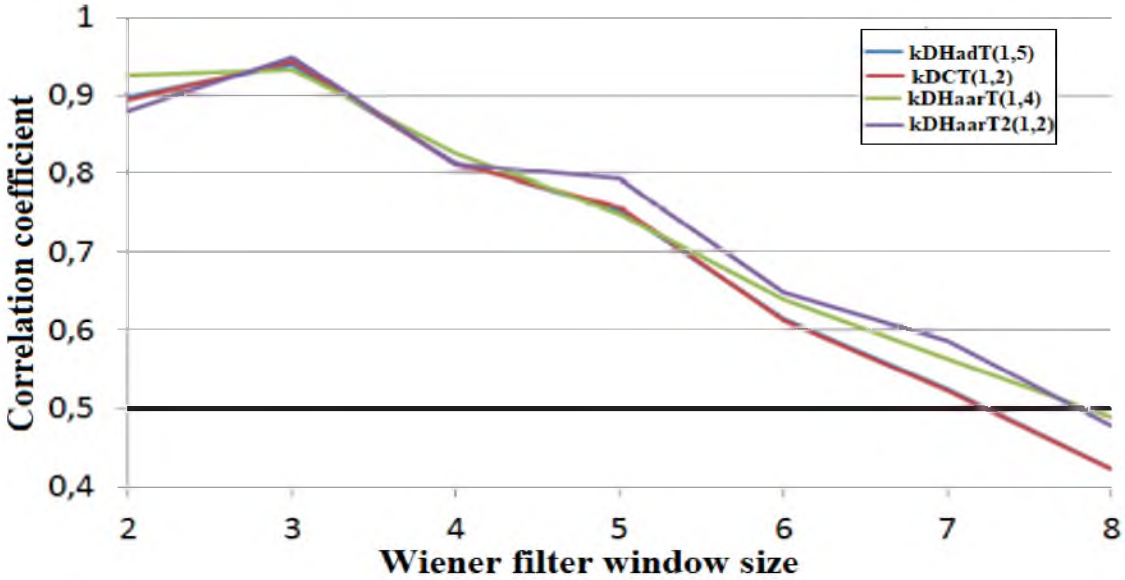


Рисунок 2.15 – Стійкість алгоритму Fami до фільтра Вінера

Встановлено, що алгоритм Fami демонструє задовільну стійкість до Вінеровської фільтрації. Використання ДКП замість ДПА забезпечить незначний приріст стійкості. Найкращі та ідентичні показники спостерігаються при використанні ДПХ першого та другого рівнів.

Одним із найбільш часто використовуваних шкідливих впливів, особливо в мережі Інтернет, є зміна розміру зображення. При моделюванні розмір стегоконтейнера пропорційно зменшувався включно до 10% початкового розміру із подальшим відновленням до початкового розміру. Результати моделювання наведено на рис. 2.16.

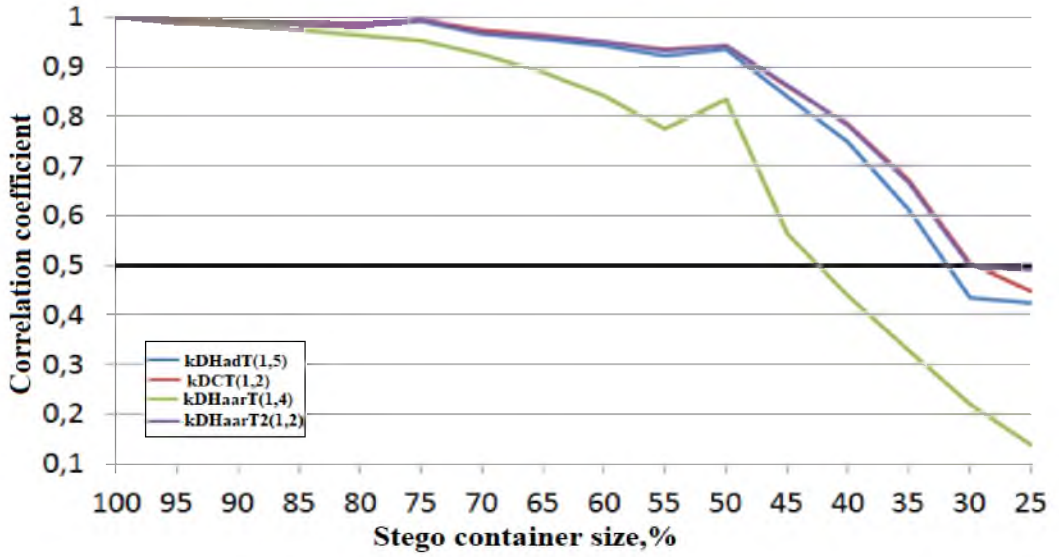


Рисунок 2.16 – Стійкість алгоритму Fami до зміни розміру зображення

Також було досліджено протидію алгоритму Fami шкідливому впливу – зміні загальної яскравості стегоконтейнера. Стійкість Алгоритму Fami до зміни яскравості стегоконтейнера представлена на рис. 2.17.

За рахунок того, що ДПА в порівнянні з іншими використовуваними перетвореннями гірше здійснює перерозподіл енергії, стійкість ЦВЗ до зміни яскравості трохи краще. Використання дворівневого ДПХ демонструє найгірші результати, що пов'язано з використанням низькочастотних коефіцієнтів для вбудовування, які зазнають найбільшої дії при подібних операціях.

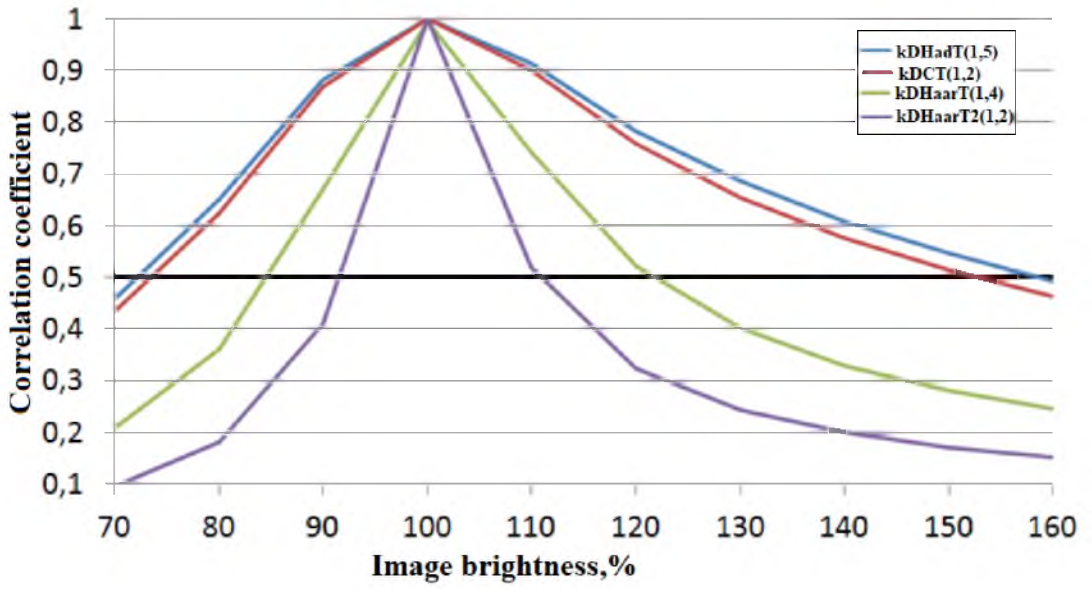


Рисунок 2.17 – Стійкість алгоритму Fami до зміни яскравості зображення

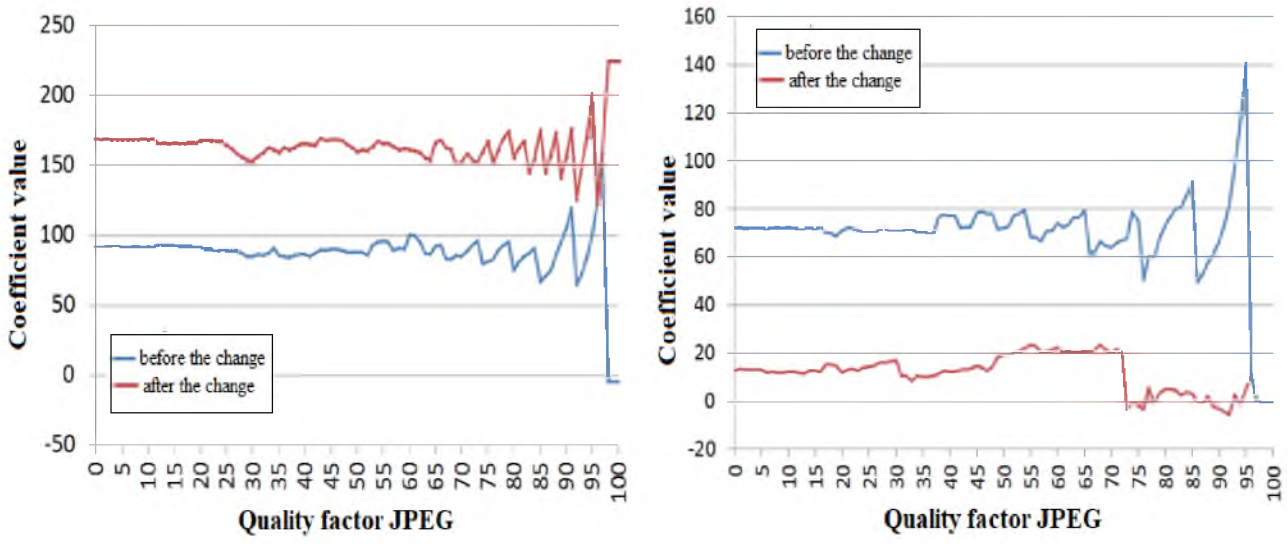
Таким чином, алгоритм Fami виявляє слабку стійкість до JPEG стиску високого рівня. Алгоритм забезпечує стійкість до Вінерівської фільтрації, але не виявляє оптимальну робастність до компресії JPEG2000, шумів Гауса та «сіль і перець». Алгоритм слабко протистоїть зміні яскравості пікселів зображення.

Результати стійкості під час використання ДПА аналогічні показникам, отриманим під час використання ДКП. При цьому підході до цифрового маркування використання ДПА є виправданим у зв'язку з низькою обчислювальною складністю, простотою апаратної реалізації та здатністю трохи збільшувати робастність ЦВЗ до зміни яскравості внаслідок поганого перерозподілу енергії зображення за допомогою ДПА. Використання ДПХ першого та другого рівнів недоцільно при даному підході через їх високу обчислювальну складність.

2.4 Стратегія вибору частотних коефіцієнтів ДПА

Для алгоритмів, подібних до Fami, для збереження інформації в процесі стиснення різниця ($a'– a$) (у разі збільшення a) або ($a– a'$) (у разі зменшення a) не повинна ставати занадто малою щодо $|w_i|$ або міняти свій знак на

протилежний (рис. 2.18). При цьому збільшення різниці допустиме, оскільки в такому випадку якість ЦВЗ знизиться набагато слабше, ніж при зменшенні різниці.



а б

Рисунок 2.18 – Зміна коефіцієнтів ДПА під час компресії JPEG після вбудовування: а – шляхом збільшення a; б – шляхом зменшення a

При вбудовуванні ЦВЗ як частотних коефіцієнтів оптимальними є два випадки. У першому випадку (рис. 2.18,а) відбувається сильна зміна значення модифікованої частотної складової a' у порівнянні з a при Q=0. Цей процес відбувається, якщо до модифікації коефіцієнта a значення $|d|/255<0.5$, а після модифікації значення $|d|/255\geq0.5$ (або навпаки).

У другому випадку (рис. 2.18,б) спостерігаємо незначне відхилення коефіцієнта a' на всьому діапазоні значень Q, що пов'язано з малим модулем вихідного коефіцієнта ДКП d, найбільш близького за частотою до a. Другий випадок небажаний при вбудовуванні найзначніших частотних коефіцієнтів ЦВЗ (DC-коефіцієнтів кожного блоку декомпозиції), проте може бути використаний при впровадженні менш значущих коефіцієнтів w_i, модуль яких $|w_i|\leq0,2$.

При вбудовуванні ЦВЗ як рядка біт оптимальним варіантом є перший випадок поведінки коефіцієнтів (рис. 2.18,а). У другому випадку (рис. 2.18,б) можливе помилкове спрацьовування стеганодетектора, оскільки немодифікований коефіцієнт ДПА при Q=0 набуває того ж значення, що й після модифікації.

На жаль, неможливо визначити значення частотного коефіцієнта d, використовуючи ДПА. Тому для цього методу необхідне використання ДКП.

Ефективність представленого підходу буде проаналізовано на прикладі модифікації алгоритму Fami, що вбудовує частотні коефіцієнти ЦВЗ.

2.5 Модифікація алгоритму Fami

Початковими параметрами алгоритму є:

• зображення-контейнер;

• бінарний водяний знак w розміром N×N;

• кількість *l* низькочастотних коефіцієнтів з таблиці *a*, взятих у порядку збільшення частотності кожного блоку декомпозиції ЦВЗ;

• пороги ентропії E_1 та E_2 для вибору блоку контейнера для вбудовування частотних коефіцієнтів ЦВЗ.

Процес вбудовування ЦВЗ поділено на 3 етапи.

Етап 1. Попередні операції.

Попередній процес скорочення вбудовуваної інформації здійснюється аналогічно до алгоритму Fami, проте для зменшення обчислювальної складності замість ДКП було використано ДПА. При цьому якість ЦВЗ знизилася незначно.

Далі створюється порожня таблиця-ключ M дескрипторів m_i, кожен з яких представлений наступними елементами:

• координати (y, x) верхнього лівого пікселя блоків декомпозиції (розміром 8×8) стегоконтейнера;

• координати модифікованого коефіцієнта a' в кожному з блоків декомпозиції стегоконтейнера для вилучення частотного коефіцієнта ЦВЗ;

• покажчик знаку коефіцієнта зміни (*sign*): «1» або «-1»;

• коефіцієнт зміни α;

• частотний коефіцієнт ДПА a початкового зображення.

Коефіцієнт зміни α_i для кожного частотного коефіцієнта w_l визначається відповідно до:

$$\alpha_i = \begin{cases} 70, \text{якщо} |w_i| \leq 1 \\ 30, \text{якщо} 1 < |w_i| \leq 3 \\ 20, \text{якщо} |w_i| > 3 \end{cases} \quad (2.10)$$

Етап 2. Процес вбудовування ЦВЗ.

Вбудовування частотних коефіцієнтів ЦВЗ здійснюється аналогічно до початкового алгоритму Fami, але з використанням представленого в розділі 2.4 методу вибору частотних коефіцієнтів ДПА. З іншого боку, для ефективного використання блоків із високою ентропією спочатку впровадженню підлягають частотні коефіцієнти $|w_i| \leq 0{,}2$.

Контейнер розбивається на блоки розміром 8×8 для кращої протидії компресії JPEG. Обчислюється ентропія блоку:

$$E = -\sum_{i=1}^{n} p_i \log_2 p_i \quad (2.11)$$

де p_i – ймовірність виникнення яскравості i. Імовірність p визначається на основі значень гістограми частот появи пікселів у блоці і знаходиться в інтервалі [0; 1]. Сума вірогідності всіх типів яскравостей блоку дорівнює 1.

Для вбудовування вибираються блоки контейнера 8×8, ентропія яких щонайменше E_1. Кожен блок піддається ДКП. В отриманій матриці коефіцієнтів ДКП здійснюється пошук коефіцієнта d_i, що задовольняє умовам:

$$\begin{cases} (d_i > c_1) \text{ і } (d_i < c_2), \text{якщо } d_i > 0 \\ (d_i > -c_2) \text{ і } (d_i < -c_1), \text{якщо } d_i < 0 \end{cases}, \quad (2.12)$$

де c_1 та c_2 – порогові значення |d|, які визначаються відповідно до виразу:

$$\begin{cases} c_1 = 50, c_2 = 80, \text{якщо } |w_i| * \alpha \geq 80 \\ c_1 = 70, c_2 = 100, \text{якщо } |w_i| * \alpha < 80 \end{cases} \quad (2.13)$$

Якщо знайдений коефіцієнт d_i задовольняє умов у (2.12), то блок пікселів піддається прямому ДПА.

Далі здійснюється модифікація частотного коефіцієнта ДПА a_i, що відповідає знайденому d_i:

$$a_i^{'} = a_i + sign * \alpha_i * w_i \ , \tag{2.14}$$

де a_i – коефіцієнт ДПА після модифікації, α_i – коефіцієнт зміни, *sign* – визначник знака впровадження, що приймає значення за наступним виразом:

$$\begin{cases} sign = 1, \text{якщо } (d_i > c_1) \text{ і } (d_i < c_2) \\ sign = -1, \text{якщо } (d_i > -c_2) \text{ і } (d_i < -c_1) \end{cases} \tag{2.15}$$

Відповідні параметри дескриптора заносяться в таблицю М. При цьому місце розташування дескриптора в таблиці відповідає місцезнаходженню частотного коефіцієнта вектор вбудовування. Блок коефіцієнтів частотних коефіцієнтів згідно (1.5) піддається зворотному ДПА в результаті виходить матриця пікселів. Елементам блоку одиничної маски, відповідним пікселям маркованого блоку, надається значення 0.

На другому етапі вбудовування здійснюється вбудовування коефіцієнтів $|w_i|$, що знаходяться в інтервалі [0; 0.2] в блоки, ентропія яких E_2 задовольняє критерію:

$$E_2 > E_1 - 2. \tag{2.16}$$

Пороги для пошуку d_i наступні: $c_1=0$, $c_2=30$.

Етап 3. Процес вилучення ЦВЗ.

Параметрами вилучення ЦВЗ є:

- контейнер та стегоконтейнер;
- ключова матриця М;
- кількість частотних коефіцієнтів L на блок декомпозиції ЦВЗ;
- кількість пікселів сторони квадратного ЦВЗ;
- розмір ЦВЗ

Вилучення ЦВЗ у вигляді вектора-рядка здійснюється наступним чином:

$$w_i = \begin{cases} (c_i^{'} - c_i)/\alpha, sign = 1 \\ (c_i - c_i^{'})/\alpha, sign = -1 \end{cases} \tag{2.17}$$

де $c_i^{'}$ – частотний коефіцієнт стегоконтейнера, c_i – частотний коефіцієнт контейнера.

Наступним етапом є процес, зворотний попередній обробці ЦВЗ. В результаті формується попередній вигляд ЦВЗ. Для запобігання можливої помилки невірного спрацьовування, вилучені пікселі піддаються бінаризації:

$$\begin{cases} w_i = 0, \text{якщо } w_i \leq 0.6 \\ w_i = 1, \text{якщо } w_i > 0.6 \end{cases} \quad (2.18)$$

2.6 Оцінка ефективності модифікованого алгоритму Fami

Оцінка ефективності модифікованого алгоритму Fami проводилась в середовищі Matlab/Simulink. Було здійснено порівняння стійкості алгоритму Fami та модифікованого алгоритму Fami по відношенню до атак компресії, зашумлення, фільтрації, зміни розміру та яскравості.

На рис. 2.19 представлено стійкість алгоритмів до стиснення JPEG. Модифікований алгоритм Fami забезпечує повну стійкість ЦВЗ до стиску JPEG. Різке падіння стійкості при Q, що знаходиться в діапазоні від 6 до 3, пов'язане з особливістю поведінки обраних коефіцієнтів при компресії JPEG.

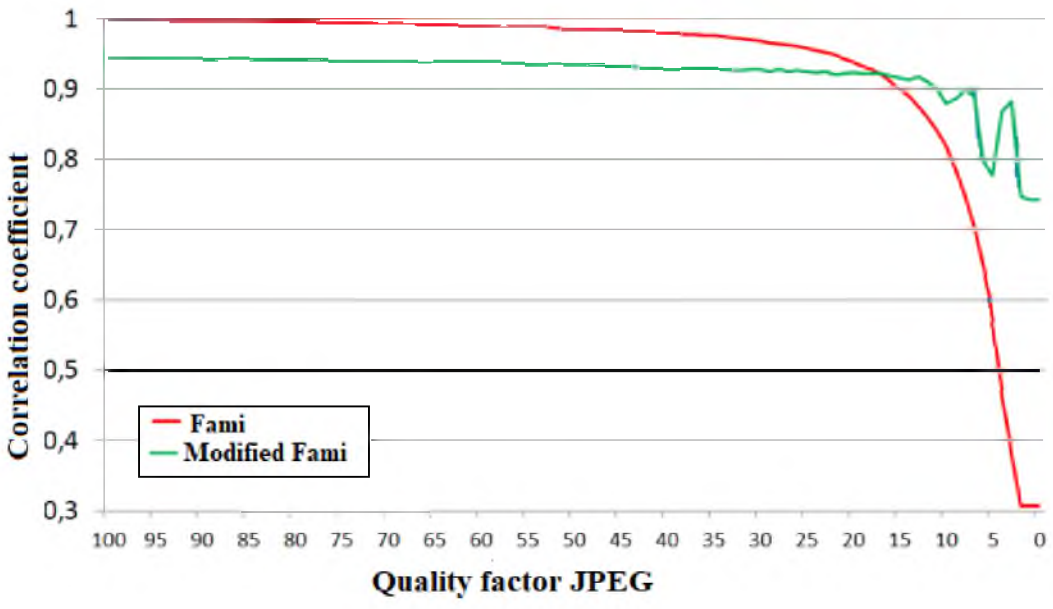


Рисунок 2.19 – Стійкість алгоритмів до стиснення JPEG

Встановлено, що модифікований алгоритм Fami у порівнянні з початковим алгоритмом демонструє практично однакову стійкість до компресії JPEG2000 – до рівня стиснення 50 (рис. 2.20).

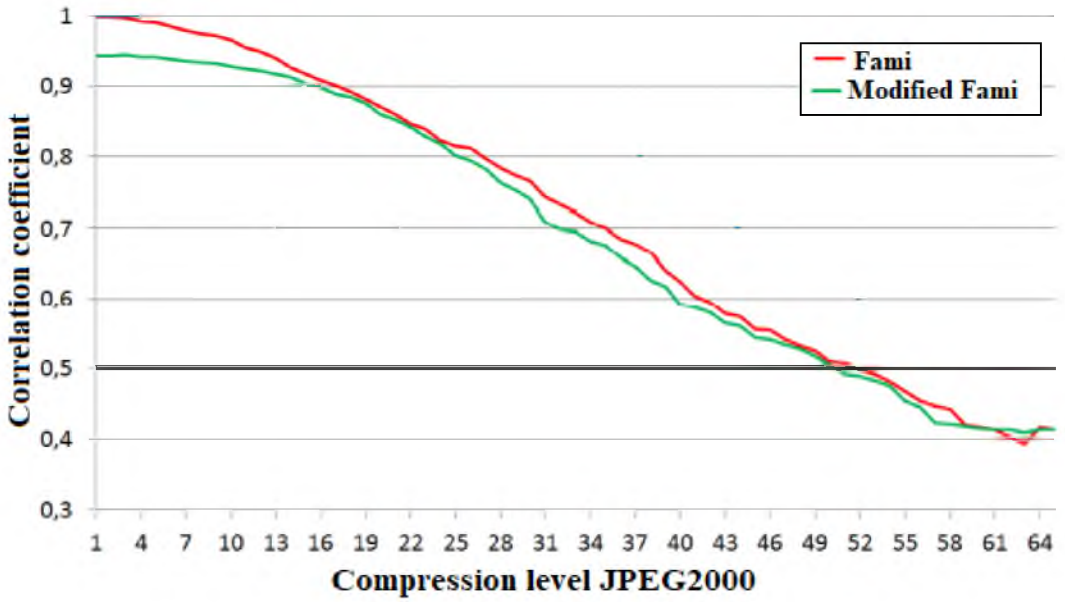


Рисунок 2.20 – Стійкість алгоритмів до компресії JPEG2000

З точки зору робастності по відношенню до шуму кращі показники демонструє модифікований алгоритм Fami у порівнянні з початковим алгоритмом Fami (рис. 2.21-2.22). ЦВЗ вилучається при Гаусовому шумі включно до рівня дисперсії 0,07, при якому зображення втрачає свою комерційну цінність.

По відношенню до шуму «сіль і перець» модифікований алгоритм Fami є стійким – ЦВЗ вилучається навіть при значенні дисперсії більше 0,1, коли зображення не представляє комерційної цінності.

Встановлено, що модифікований алгоритм Fami у порівнянні з початковим алгоритмом демонструє практично однакову стійкість до фільтрації Вінера (рис. 2.23). Модифікація Fami дозволила розпізнавати вбудований ЦВЗ при розмірі вікна фільтрації 8×8.

Встановлено, що модифікований алгоритм Fami має найгіршу стійкість до зміни розміру у порівнянні з початковим алгоритмом (рис. 2.24). ЦВЗ

виявляє стійкість за зміни розміру контейнера до 40%. На діапазоні від 100% до 40% стійкість нижча, ніж у початкового алгоритму.

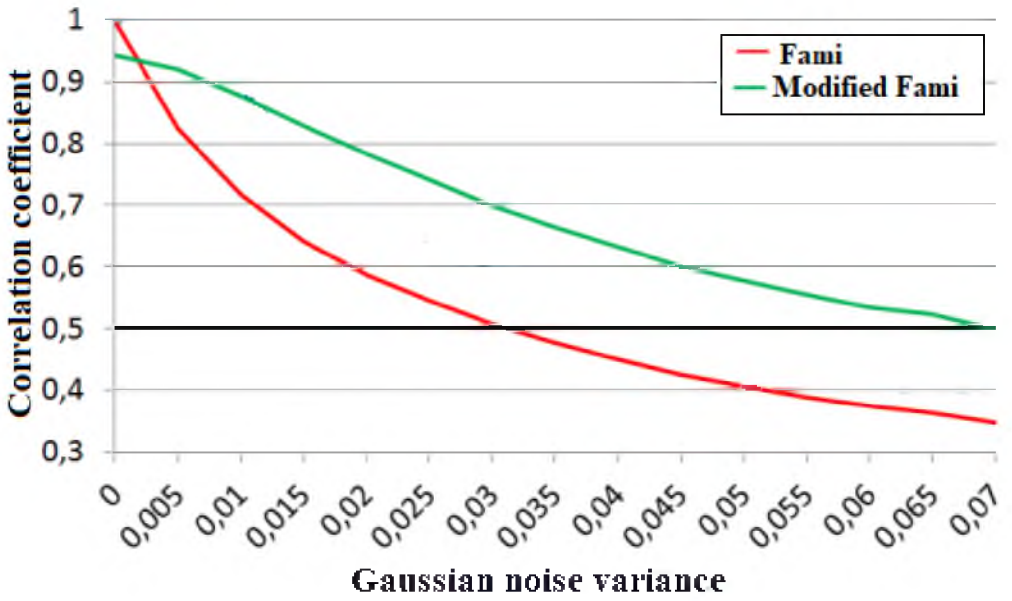


Рисунок 2.21 – Стійкість алгоритмів до шуму Гауса

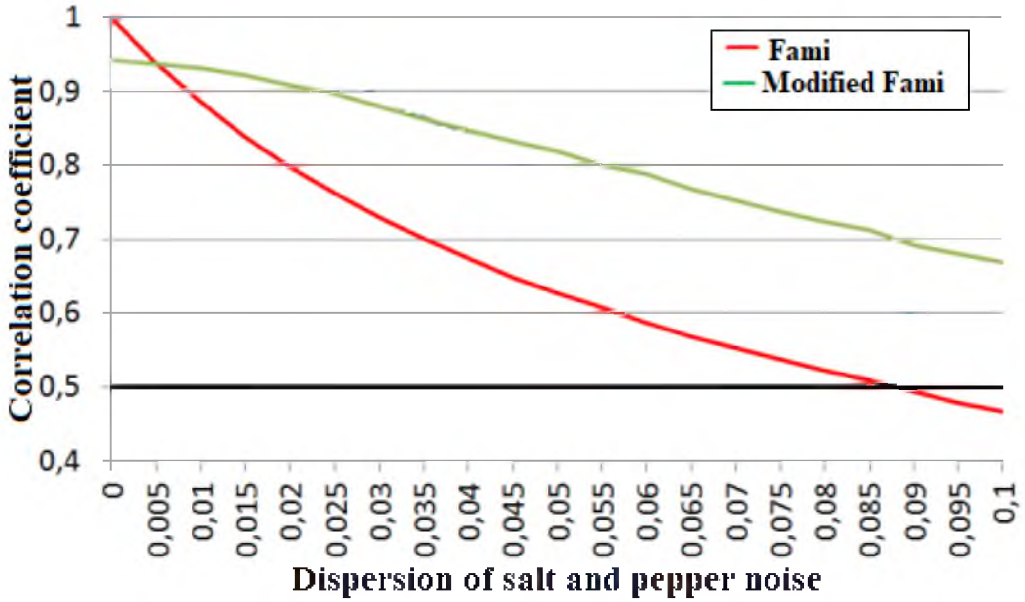


Рисунок 2.22 – Стійкість алгоритмів до шуму «сіль і перець»

Також модифікований алгоритм Fami було протестовано на стійкість до зміни яскравості стегоконтейнера (рис. 2.25). Встановлено, що модифікація алгоритму Fami має великий діапазон стійкості до зміни яскравості контейнера: від 60% до 260% від початкової яскравості.

Рисунок 2.23 – Стійкість алгоритмів до фільтрації Вінера

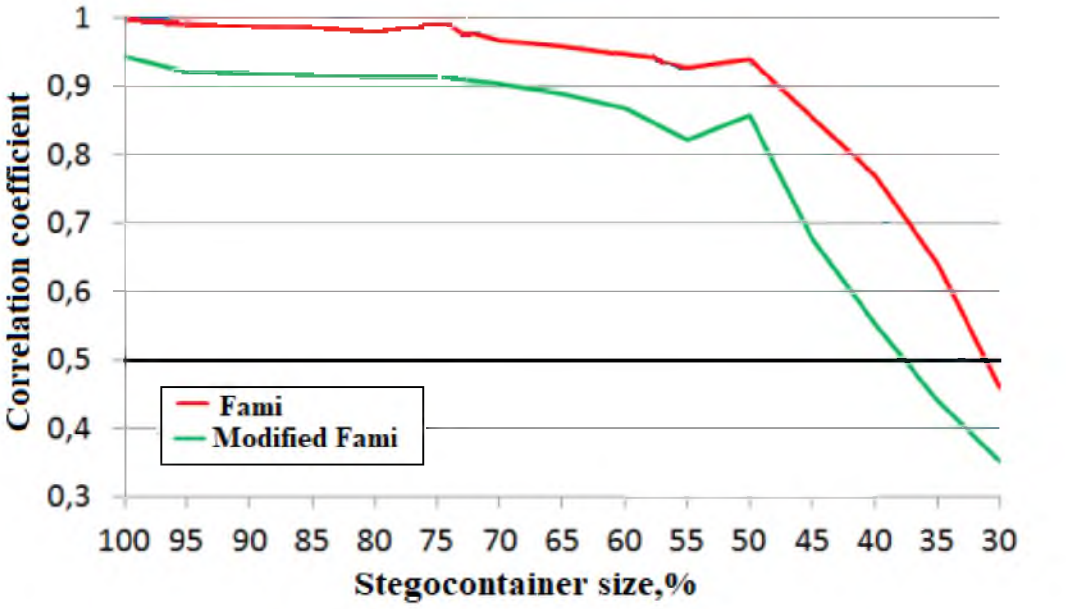


Рисунок 2.24 – Стійкість алгоритмів до зміни розміру стегоконтейнера

Таким чином, якщо до ЦВЗ пред'являється вимоги підвищеної стійкості до зашумлення, найкращим є модифікація алгоритму Fami. Оскільки модифікований алгоритм залежить від параметра ентропії, стійкість ЦВЗ безпосередньо залежить від кількості складних текстур у контейнері, оскільки, чим вище рівень ентропії, тим більші коефіцієнти посилення можна використовувати для вбудовування ЦВЗ. Отже, модифікований алгоритм, як і

Fami найбільш придатні для контейнерів з великою кількістю складних текстур. В іншому випадку необхідне сильне зменшення кількості інформації, що вбудовується, для збереження її стійкості.

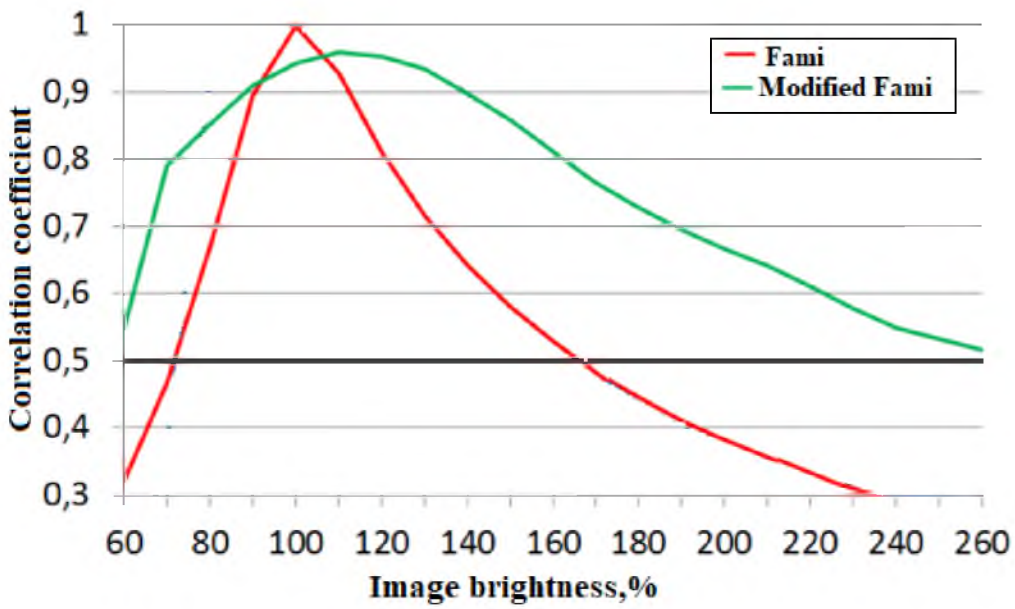


Рисунок 2.25 – Стійкість алгоритмів до зміни яскравості стегоконтейнера

2.7 Висновок

Досліджено взаємозалежність між коефіцієнтами ДПА та ДКП, в результаті вдалося визначити найбільш близькі до ДКП низькочастотні компоненти ДПА.

Визначено область стійкості алгоритму Fami для шкідливих впливів різного типу.

Встановлено, що використання перетворення Адамара здатне сильно знизити обчислювальну складність алгоритмів цифрового маркування, забезпечуючи стійкість ЦВЗ, подібну до стійкості при використанні ДКП.

Наведена стратегія вибору частотних коефіцієнтів для вбудовування водяного знаку забезпечує збільшення стійкості до сильного стиску JPEG. При

використанні даної стратегії переважно вбудовування бінарного зображення, перетвореного на послідовність біт.

Запропоновано модифікацію алгоритму Fami, що забезпечує підвищену стійкість до шуму Гауса та до шуму «сіль і перець». Встановлено, що якщо до ЦВЗ пред'являється вимоги підвищеної стійкості до зашумлення, слід використовувати модифікацію алгоритму Fami.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності запропонованого підходу до стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів. Для досягнення цієї необхідно здійснити наступні розрахунки: капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування; річний економічний ефект від впровадження запропонованих заходів; показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу щодо стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів, $t_{тз}=20$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=32$;

t_a – тривалість аналізу існуючих загроз безпеки інформації, $t_a=60$;

t_p – тривалість розробки підходу щодо стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів, $t_м=48$;

$t_д$ – тривалість підготовки технічної документації, $t_д=10$.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 20+32+60+48+10 = 170 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 36550 + 1123{,}7 = 37673{,}7 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 170*215 = 36550 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 170*6{,}61 = 1123{,}7 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{зпч} = 0{,}9 \cdot 3 \cdot 1{,}68 + \frac{8600 \cdot 0{,}25}{1920} + \frac{9200 \cdot 0{,}2}{1920} = 6{,}61 \text{ грн.}$$

Для реалізації запропонованого підходу може бути використано стандартне апаратне забезпечення, яке вже наявне на підприємстві, тому капітальні витрати не виникають.

Оцінка ефективності запропонованого підходу щодо стеганографічного вбудовування цифрового водяного знака в завірене повідомлення проведена шляхом моделювання в середовищі Matlab / Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 1000 грн.

Вирішення певних технічних завдань із збільшення скритності і точності відновлення приховуваного сигналу потребує залучення аутсорсингових організації, вартість послуг котрих складає 16000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$= 37673,7 + 16000 + 1000 = 54673,7 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

де $С_в$ – вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Середовище Matlab/Simulink, яке застосовується для оцінки ефективності запропонованого підходу щодо стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів, вже використовується на підприємстві, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 10000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18000 грн. Додаткова заробітна плата – 5% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,15 ставки. Отже,

$$С_з = (18000*12 + 18000*12*0,05)*0,15 = 34020 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 34020*0,22 = 7484,4 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,9*4*1920*1,68 = 11612,16 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 54673,7*0,01 = 546,74 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 10000+34020+7484,4+11612,16 +546,74 = 63663,3 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 30%. Тому:

$$С_{ак}= 54673,7*0,3=16402,11 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 63663,3 + 16402,11 = 80065,41 \text{ грн.}$$

3.2 Оцінка можливого збитку

Запропонований підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю відноситься до техніки захисту справжності повідомлень, таких як перетворені до цифрового

вигляду мовні, звукові, музичні, телевізійні, факсимільні і подібні повідомлення. Технічним результатом, що досягається при реалізації запропонованого рішення, є розробка підходу до формування і перевірки завіреного ЦВЗ повідомлення, що забезпечує підвищення захищеності повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

Формування і перевірку завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю може бути використано для встановлення справжності мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, переданих і збережених в сучасних інформаційно-телекомунікаційних системах.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

При порушенні прав інтелектуальної власності на мовні, звукові, музичні, телевізійні, факсимільні і інших мультимедійні повідомлення, передані і збережені в сучасних інформаційно-телекомунікаційних системах, величина можливого збитку може бути визначена відповідно до розміру відшкодування завданих збитків, що визначається правом інтелектуальної власності, зокрема Цивільним кодексом України, Кримінальним кодексом України, ВСУ від 31.03.95 р. №4 «Про судову практику у справах про відшкодування морального (немайнового) збитку» тощо. У разі встановлення величини компенсації за завдану шкоду підприємству, яка виникла внаслідок недостатнього рівня захищеності його об'єктів інтелектуальної власності, а саме мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, величину можливого збитку можна встановити наступним чином:

$$B = n * R * F$$

де n – кількість мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, що потребує захисту;

R – середнє значення можливості реалізації ризику порушень прав інтелектуальної власності;

F – середнє значення можливого штрафу за законодавством України (ВСУ від 31.03.95 р. № 4 «Про судову практику у справах про відшкодування морального (немайнового) збитку»).

При кількості зображень мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, що потребує захисту, 60 одиниць, вірогідності реалізації ризику, яка дорівнює 30% (R=0,3) та величині штрафу за порушення прав інтелектуальної власності, який дорівнюватиме 22000 грн., величина можливого збитку складе:

$$B=60*0,3*22000=396000 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де В – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації загрози (25%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 396000 - 80065,41 = 315934,59 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{315934,59}{54673,7} 5,78, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$5,78 > (6 - 5)/100 = 5,78 > 0,01.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{5,78} = 0,17 \text{ років.}$$

3.4 Висновок

Отже, згідно з наведеними розрахунками можливо зробити висновок, що розробка підходу щодо стеганографічного впровадження інформації в цифрові зображення за допомогою частотних методів є економічно доцільною. Капітальні витрати, які складають 54673,7 грн, дозволяють отримати ефект величиною 315934,59 грн. Відповідно до отриманих значень показників

економічної можна зазначити, що такий підхід дозволить отримувати 5,78 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт повернення інвестицій ROSI складає 5,78 грн).

Величина економічного ефекту визначатиметься також розміром компанії, величиною вартості нематеріальних активів (об'єктів прав інтелектуальної власності) та кількістю об'єктів прав інтелектуальної власності, право на авторство яких може бути порушеним.

ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

1. Проведено класифікацію алгоритмів цифрового маркування нерухомих зображень, з яких частотні алгоритми цифрового маркування є найбільш підходящими для протидії атак компресії.

2. Найбільш перспективним перетворенням є дискретне перетворення Адамара, використовуючи яке ЦВЗ здатний протистояти незалежній від платформи компресії (JPEG або JPEG2000).

3. При використанні сингулярного розкладання в алгоритмах цифрового маркування необхідна ретельна перевірка на наявність помилкового спрацьовування стеганодетектора.

4. Обґрунтована методика тестування алгоритмів цифрового маркування: вибрано типи контейнера та ЦВЗ, визначено вхідні параметри та метрики аналізу якості.

5. Досліджено взаємозалежність між коефіцієнтами ДПА та ДКП, в результаті вдалося визначити найбільш близькі до ДКП низькочастотні компоненти ДПА.

6. Визначено область стійкості алгоритму Fami для шкідливих впливів різного типу.

7. Встановлено, що використання перетворення Адамара здатне сильно знизити обчислювальну складність алгоритмів цифрового маркування, забезпечуючи стійкість ЦВЗ, подібну до стійкості при використанні ДКП.

8. Наведена стратегія вибору частотних коефіцієнтів для вбудовування водяного знаку забезпечує збільшення стійкості до сильного стиску JPEG. При використанні даної стратегії переважно вбудовування бінарного зображення, перетвореного на послідовність біт.

9. Запропоновано модифікацію алгоритму Fami, що забезпечує підвищену стійкість до шуму Гауса та до шуму «сіль і перець». Встановлено, що якщо до

ЦВЗ пред'являється вимоги підвищеної стійкості до зашумлення, слід використовувати модифікацію алгоритму Fami.

ПЕРЕЛІК ПОСИЛАНЬ

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

2. Хорошко В.О., Азаров О.Д., Шелест М.Э., Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов. – Винница: ВДТУ, 2003.-143 с.

3. Конахович Г.Ф. Компьютерная стеганография: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

4. Булдакова, Т.И Оценка эффективности защиты систем электронного документооборота / Т.И. Булдакова, Б.В. Глазунов, Н.С. Ляпина // Доклады ТУСУРа. – 2012. – № 1 (25), часть 2. – С. 52-56.

5. Коробейников А.Г. Цифровые водяные знаки в графических файлах / А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – № 1 (83). – С. 152-157.

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

7. Osborne, C.F. A Digital Watermark / C.F. Osborne, R.V. Schyndel, A.Z. Tirkel // IEEE Intern. Conf. on Image Processing. – 1994. – pp. 86-90.

8. Phizmann B. Information Hiding Terminology / B. Phizmann // Information Hiding, Springer Lecture Notes in Computer Science. – 1996. – Vol. 1174. – pp. 347-350.

9. Савчина Е.И. Встраивание цифровых водяных знаков в частотную и пространственную области изображения / Е.И. Савчина // Вестник СибГАУ. – Том 17, № 3. – 2016. – С. 631-637.

10. Westfeld A. Attacks on steganographic systems / A. Westfeld, A. Pfitzmann // Proc. of Information Hiding, Third Int. Workshop, Dresden, Germany. – September 28- October 1. – 1999. – P. 61-75.

11. Fridrich J. Practical steganalysis of digital images-state of the art / J. Fridrich, M. Goljan // Proc. SPIE Photonics West, Electronic Imaging (2002), Security and Watermarking of Multimedia Contents, San Jose, CA. – January 2002. – vol. 4675. – P. 1-13.

12. Dumitrescu S. A new framework of LSB steganalysis of Digital Media / S. Dumitrescu, X. Wu // IEEE Trans. Signal Process. – October 2005. – Vol. 53, no. 10. – P. 3936-3947.

13. Hartung F. Multimedia Watermarking Techniques / F. Hartung, M. Kutter // IEEE Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information. – July 1999. – Vol. 87, no. 7. – P. 1079-1107.

14. Zhao X. Introduction to Robust Transform Based Image Watermarking Techniques / X. Zhao, T. S. Ho Anthony // Intelligent Multimedia Analysis for Security Applications. – 2010. – Vol. 282. – P. 337-364.

15. Tanha M. An Overview of Attacks against Digital Watermarking and their Respective Countermeasures / M. Tanha, S.D.S. Torshizi, M.T. Abdullah, F. Hashim // IEEE Published Proceeding in International Cyber Security Conference (CyberSec 2012). – 2012. – P. 265-270.

16. Тропченко А.Ю. Методы сжатия изображений, аудиосигналов и видео. Учебное пособие. / А.Ю. Тропченко, А.А. Тропченко. – Государственный университет ИТМО. – Санкт-Петербург, 2009. – 108 с.

17. Zhang H. Image watermarking based on an iterative phase retrieval algorithm and sine-cosine modulation in the discrete-cosine-transform domain / H. Zhang, L.Z. Cai, X.F. Meng, X.F. Xu, X.L. Yang, X.X. Shen, G.Y. Dong // Optic Communications – 2007. – Vol. 278. – P. 257-263.

18. Fakhari P. Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach / P. Fakhari, E. Vahedi, C. Lucas // Digital Signal Processing. – 2011. – Vol. 21, Issue 3. – P. 433-446.

19. Maity S.P. Perceptually adaptive spread transform image watermarking scheme using Hadamard transform / S.P. Maity, M.K. Kundu // Information Sciences. – 2011. – Vol. 181. – P. 450-465.

20. Santi P. Maity, Malay K. Kundu DHT domain digital watermarking with low loss in image informations // Int. J. Electron. Commun. – 2010. – Vol. 64. – P. 243-257.

21. Anthony T.S. Robust digital image-image watermarking algorithm using fast Hadamard transform / T.S. Anthony, J. Shen, A.K.K. Chow, J. Woon // International Symposium on circuits and systems. – May 2003. – Vol. 3. – P. 826-829.

22. Saryazdi S. A Blind Digital Watermark in Hadamard Domain / S. Saryazdi, H. Nezamabadi // World Academy of Science, Engineering and Technology. – 2005. – Vol. 3 – P. 245-248.

23. Разинков Е.В. Встраивание цифрового водяного знака в изображение с использованием комплексного преобразования Адамара. / Е. В. Разинков, Р.Х. Латыпов // Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. – 25-26 октября 2006 г. – М.: МЦНМО, 2006. – 660 с.

24. Zhang Y. A blind Image Watermarking Scheme Using Fast Hadamard Transform / Y. Zhang, Z.M. Lu, D.N. Zhao // Information Technology Journal. – 2010. – Vol. 9, no. 7. – P. 1369-1375.

25. Latif A.A Watermarking Scheme Based on the Parametric Slant-Hadamard Transform / A.A. Latif //Journal of Information Hiding and Multimedia Signal Processing. – 2011. – Vol. 2, no. 4. – P. 377-389.

26. Anthony T.S. A Character-Embedded Watermarking Algorithm Using the Fast Hadamard Transform for Satellite Images / T.S. Anthony, J. Shen, S.H. Tan // SPIE Proceedings. – 2003. – Vol. 4793. – P. 156-167.

27. Sarker Md.I.H. An Efficient Image Watermarking Scheme Using BFS Technique Based on Hadamard Transform / Md.I.H. Sarker Md. I.H., M.I. Khan M.I. // Smart Computing Review. – 2013. – Vol. 3, no. 5. – P. 298-308.

28. Bhatnagar G. Robust Watermarking in Multiresolution Walsh-Hadamard Transform / G. Bhatnagar, B. Raman // 2009 IEEE International Advance Computing Conference (IACC 2009), 6-7 March. – 2009. – P. 894-899.

29. Shabanali Fami E. Adaptive watermarking in Hadamard transform coefficients of textured image blocks / E. Shabanali Fami, S. Samavi, H. Rezaee Kaviani, Z. Molaei Radani // 16th International Symposium on Artificial Intelligence and Signal Processing. Shiraz, Iran. – 2012. – Vol. 2012. – P. 503-507.

30. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – Москва: Техносфера. – 2004. – 368 с.

31. Cox I.J. Secure spread spectrum watermarking for multimedia / I.J. Cox, J. Kilian, T. Leighton, T.G. Shamoon // Proceedings of the IEEE International Conference on Image Processing. – 1997. – Vol. 6. – P. 1673-1687.

32. Kornblum J.D. Using JPEG quantization tables to identify imagery processed by software / J.D. Kornblum // Digital Investigation. – 2008, vol. 5. – P. 521-525.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	23	
6	А4	Спеціальна частина	31	
7	А4	Економічний розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Левераш.ppt

2 Диплом Левераш.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-20-1 Левераша В.С.

на тему: «Стеганографічне впровадження інформації в цифрові зображення за допомогою частотних методів»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 83 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення стійкості цифрових водяних знаків, що вбудовуються в графічні зображення, до різноманітних атак, таких як JPEG стиск, зашумлення, фільтрація тощо.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу основ цифрового маркування нерухомих зображень та обзору стегоалгоритмів, що ґрунтуються на ДПА, в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було досліджено взаємозалежність між коефіцієнтами ДПА та ДКП; наведено стратегію вибору частотних коефіцієнтів для вбудовування ЦВЗ; запропоновано модифікацію відомого алгоритму цифрового маркування і оцінено його ефективність.

Практична цінність роботи полягає в тому, що впровадження розглянутих підходів дозволить окремим авторам і Інтернет магазинам вбудовувати ЦВЗ високого рівня стійкості до зашумлення для захисту авторських прав на свою продукцію.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Левераш В.С. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**