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 бакалавра

студента *Астахов Олександр Олегович*

академічної групи *125-18зск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів*

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
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Астахов Олександр Олегович* **академічної групи** *125-18зск-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 27.04.2021р № 234-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів впровадження інформації у нерухомі зображення і вейвлет-перетворень, а також існуючих підходів до вбудовування додаткової інформації у цифрові зображення.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації та оцінка його ефективності.	01.04.2021 – 12.05.2021
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2021 – 09.06.2021

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Астахов О.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 16 рис., 4 додатки, 39 джерел.

Об’єкт розробки – цифрові зображення формату JPEG 2000.

Предмет розробки – підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000.

Мета кваліфікаційної роботи – зменшення оцінки рівня спотворень цифрового зображення формату JPEG 2000.

Наукова новизна результатів полягає у можливості вбудовування конфіденційної інформації із різним ступенем стійкості до стеганоаналізу при відсутності необхідності в зміні статистичних характеристик розподілу вейвлет-коефіцієнтів. Для забезпечення найбільшої ефективності вбудовування в цифрове зображення повідомлення останньому надається характер псевдовипадкової послідовності.

У першому розділі проаналізовано принципи впровадження інформації у нерухомі зображення і вейвлет-перетворень, а також існуючі підходи до вбудовування додаткової інформації у цифрові зображення.

У спеціальній частині роботи запропоновано підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.

КОЕФІЦІЄНТ СТИСНЕННЯ, ДИСКРЕТНЕ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ, КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ, ЦИФРОВЕ ЗОБРАЖЕННЯ, ПСЕВДОВИПАДКОВА ПОСЛІДОВНІСТЬ, ПІКОВЕ ВІДНОШЕННЯ СИГНАЛУ ДО ШУМУ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 73 с., 16 рис., 4 приложения, 39 источников.

Объект разработки – цифровые изображения формата JPEG 2000.

Предмет разработки – подход к стеганографическому встраиванию сообщения в цифровое изображение формата JPEG 2000.

Цель квалификационной работы – уменьшение оценки уровня искажений цифрового изображения формата JPEG 2000.

Научная новизна заключается в возможности встраивания конфиденциальной информации с разной степенью устойчивости к стеганоанализу при отсутствии необходимости в изменении статистических характеристик распределения вейвлет-коэффициентов. Для обеспечения наибольшей эффективности встраивания в цифровое изображение сообщения последнему придается характер псевдослучайной последовательности.

В первой главе проанализированы принципы внедрения информации в неподвижные изображения и вейвлет-преобразований, а также существующие подходы к встраивания дополнительной информации в цифровые изображения.

В специальной части работы предложен подход к стеганографическому встраиванию сообщения в цифровое изображение в формате JPEG 2000 с сохранением целостности внедренной информации и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, затрат на эксплуатацию системы безопасности и срок окупаемости инвестиций применения предложенного подхода.

КОЭФФИЦИЕНТ СЖАТИЯ, ДИСКРЕТНОЕ ВЕЙВЛЕТ ПРЕОБРАЗОВАНИЕ, КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ, ЦИФРОВОЕ ИЗОБРАЖЕНИЕ, ПСЕВДОСЛУЧАЙНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, ПИКОВОЕ ОТНОШЕНИЕ СИГНАЛА К ШУМУ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 73, fig. 16, 4 additions, 39 sources.

The object of development is JPEG 2000 digital images.

The subject of development is the approach to steganographic embedding of a message in a JPEG 2000 digital image.

The purpose of the qualification work is to reduce the assessment of the level of distortion of a digital image in the JPEG 2000 format.

Scientific novelty lies in the possibility of embedding confidential information with varying degrees of resistance to steganalysis without the need to change the statistical characteristics of the distribution of wavelet coefficients. To ensure the highest efficiency of embedding a message into a digital image, the latter is given the character of a pseudo-random sequence.

The first chapter analyzes the principles of embedding information in still images and wavelet transforms, as well as existing approaches to embedding additional information in digital images.

In a special part of the work, an approach to steganographic embedding of a message into a digital image in JPEG 2000 format with preserving the integrity of the embedded information is proposed, and its effectiveness is evaluated. Based on the results of the research, conclusions were drawn regarding the solution of the task.

In the economic section, calculations of capital costs, costs of operating the security system and the payback period of the application of the proposed approach.

COMPRESSION RATIO, DISCRETE WAVELET CONVERSION, COMPUTER STEGANOGRAPHY, DIGITAL IMAGE, PSEUDO RANDOM SEQUENCE, PEAK SIGNAL TO NOISE RATIO, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВП – Вейвлет-перетворення;

ДВП – Дискретне вейвлет-перетворення;

ДКП – Дискретне косинус-перетворення;

ДПФ – Дискретне перетворення Фур'є;

ПВП – Псевдовипадкова послідовність;

ПКЛ – Перетворення Карунена-Лоєва;

СЛЗ – Система людського зору;

ЦВЗ – Цифровий водяний знак;

ШВП – Швидке вейвлет перетворення;

JPEG 2000 – Стандарт стиснення зі втратами для повнокольорових зображень на основі алгоритму дискретного вейвлет перетворення;

PSNR – Peak Signal-to-Noise Ratio – Співвідношення між максимумом можливого значення сигналу і потужністю шуму, що спотворює значення сигналу.

ЗМІСТ

ВСТУП

Наразі, незважаючи на велику кількість існуючих методів і алгоритмів маркування, не існує універсального способу захисту зображень і визначення його автентичності, тому завдання розробки моделей і алгоритмів, що дозволяють забезпечити можливість докази автентичності та справжності захищених зображень, є актуальною.

Розробка різних методів і заходів щодо захисту інформації ведеться з найдавніших часів. Серед них можна виділити два основних напрямки – криптографія і стеганографія. Криптографія забезпечує приховування вмісту повідомлень за рахунок їх шифрування, а стеганографія – приховування самого факту існування секретних даних при їх передачі, зберіганні або обробці [1-5].

Розробка методів стеганографічного захисту інформації багатьма вченими відбувалась без врахування взаємозв'язку вимог таємності та робастності. Порушення таємності призводить до повної втрати стеганографічної захищеності даних. Саме зазначена якість задає основні обмеження при застосуванні стеганографічних перетворень, що передбачають можливість пасивних атак. Забезпечення якості таємності в більшості робіт визначає можливість стеганографічного зображення (стегозображення) залишитися непоміченим, що відповідає показнику ймовірності (або ентропії) правильного детектування методами стеганографічного аналізу (стеганоаналізу). Другим важливим аспектом є вимога робастності, яка визначається ентропією таємних даних при витяганні, що відповідає пропускній здатності двійкового каналу. Така якість задає додаткові обмеження при використанні стеганографічних перетворень, що передбачають можливість активних атак. Показники якостей таємності та робастності залежать від особливостей стегоконтейнера, використовуваного перетворення, методу вбудовування тощо [1-12].

Напрямок в області цифрової обробки сигналів, який наразі успішно розвивається, і що виник в кінці минулого століття, спричинив за собою

зростання наукового інтересу до теорії і техніки обробки сигналів, зображень та часових рядів. Цей напрямок отримав назву вейвлет перетворення (ВП). ВП – це потужний засіб аналізу і обробки сигналів, і здатний повністю замінити обробку сигналів традиційними методами.

Наразі вейвлети широко застосовуються для розпізнавання образів; при обробці і синтезі різних сигналів, наприклад мовних, медичних; для вивчення властивостей турбулентних полів і в багатьох інших випадках. Особливо великий розвиток отримала практика застосування вейвлетів для вирішення завдань стиснення і обробки зображень, що є нестаціонарними за своєю природою. У цій області застосування вейвлет-перетворення дозволило досягти одночасного зниження складності та підвищення ефективності кодерів. Ядром міжнародних стандартів зі стиснення нерухомих зображень і відео – JPEG2000 і MPEG-4 є вейвлет-перетворення.

Таким чином, вдосконалення підходів до стеганографічного вбудовування інформації у цифрові зображення із використанням вейвлет фільтрів наразі є актуальною задачею.

Метою роботи є зменшення оцінки рівня спотворень цифрового зображення формату JPEG 2000.

Постановка задачі:

• проаналізувати принципи впровадження інформації у нерухомі зображення, а також вейвлет-перетворень;

• провести аналіз існуючих підходів до вбудовування додаткової інформації у цифрові зображення;

• запропонувати підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Впровадження інформації у нерухомі зображення

1.1.1 Практичні аспекти побудови стеганографічних систем

Стеганографічна система (стеганосистема) – це сукупність засобів і методів, які використовуються для формування прихованого каналу передачі інформації [1-5]. Стеганосистема складається з таких основних елементів, наведених на рис. 1.1:

• прекодер – пристрій, призначений для перетворення приховуваного повідомлення до виду, зручного для вбудовування в сигнал-контейнер;

• контейнер – інформаційна послідовність, у якій ховається повідомлення;

• стеганокодер – пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані із урахуванням їх моделі;

• пристрій виділення убудованого повідомлення;

• стеганодетектор – пристрій, призначений для визначення наявності стегоповідомлення;

• декодер – пристрій, що відновлює приховане повідомлення (цей вузол може бути відсутнім).

На рис. 1.2 наведена класифікація систем цифрової стеганографії. Стеганосистема утворює стеганоканал, по якому передається заповнений контейнер. Цей канал уважається підданим впливам з боку порушників. Відповідно можна виділити три типи порушників, яким повинна протистояти стеганосистема: пасивний, активний і злочинний порушники. Слід зазначити, що пасивний зловмисник може бути лише в стеганосистемах прихованої передачі даних. Для систем ЦВЗ характерні активні та злочинні порушники.

Для того щоб стеганосистема була надійною, необхідне виконання при її проектуванні ряду вимог.

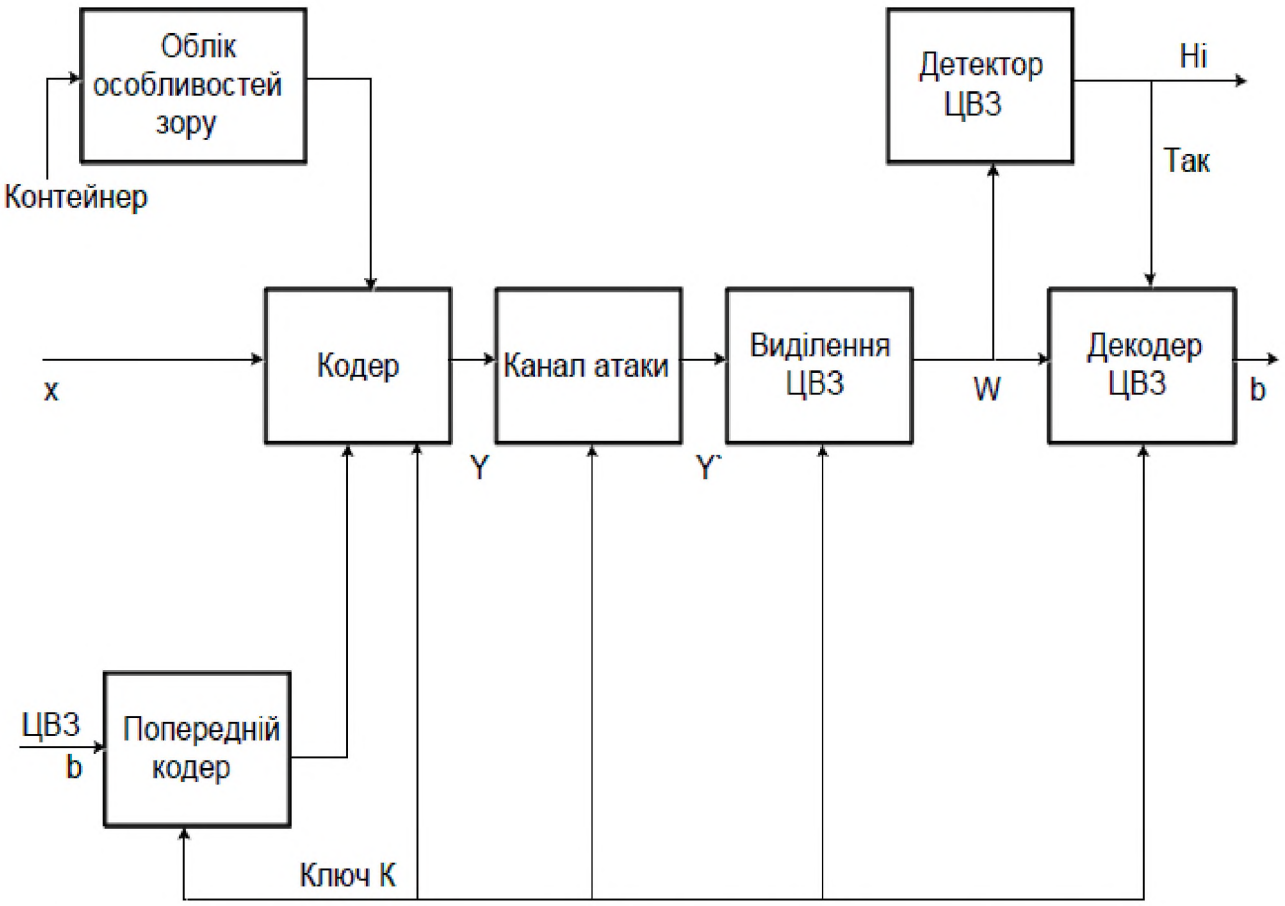

Рисунок 1.1 – Структурна схема типової стеганосистеми цифрових водяних знаків (ЦВЗ)

Безпека системи повинна повністю визначатися таємністю ключа. Це означає, що зловмисник може повністю знати всі алгоритми роботи стеганосистеми та статистичні характеристики множин повідомлень і контейнерів, і це не дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері.

Знання зловмисником факту наявності повідомлення в будь-якому контейнері не повинне допомогти йому при виявленні повідомлень в інших контейнерах.

Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення у візуально незначущі множини сигналу. Однак ці ж множини використовують і алгоритми стиску. Тому, якщо зображення буде надалі піддаватися стиску, то приховане повідомлення може зруйнуватись.

Отже, біти повинні вбудовуватися у візуально значущі множини, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра.

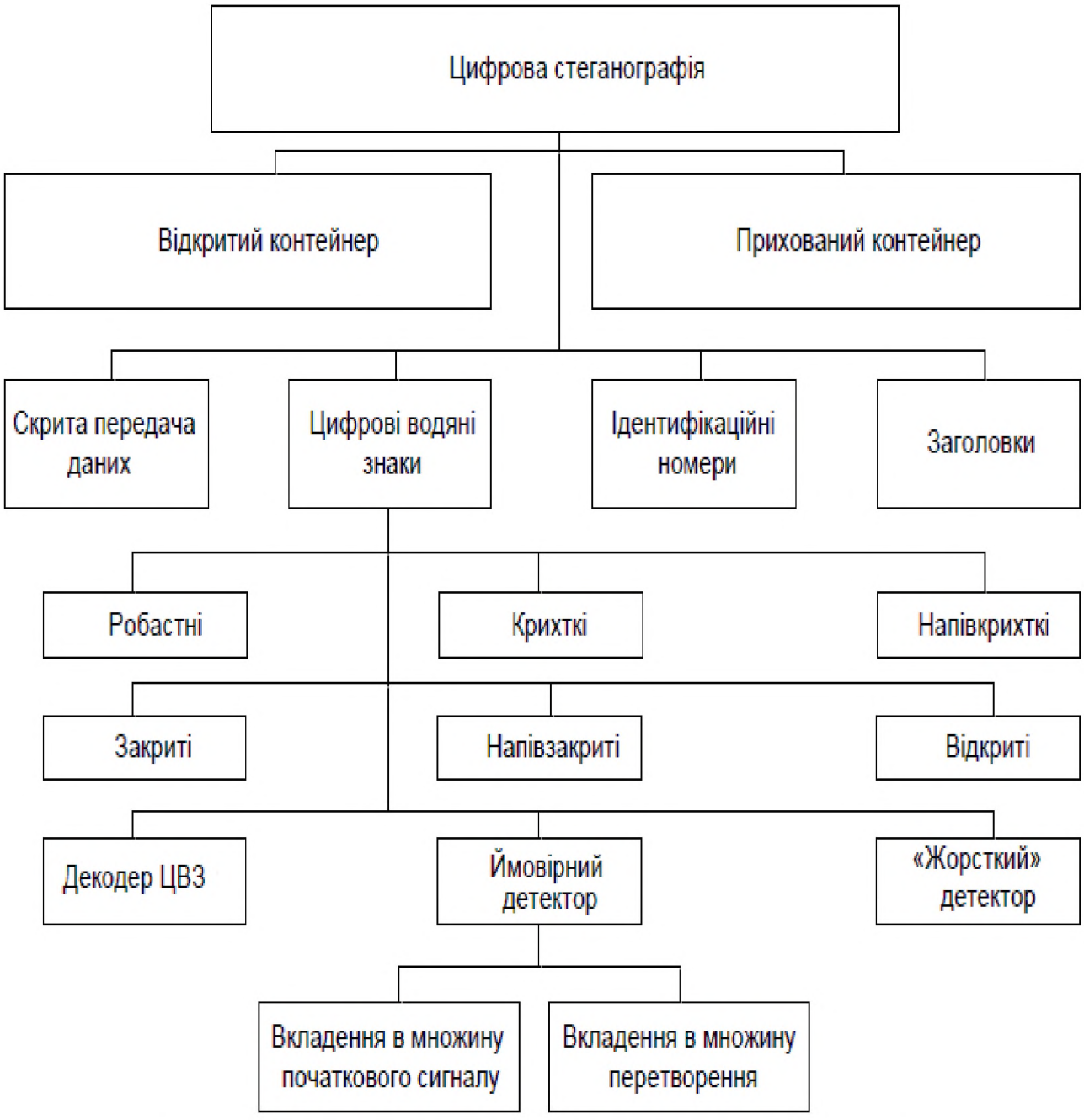

Рисунок 1.2 – Класифікація систем цифрової стеганографії

Стеганосистема повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не утримує.

Повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна, в основному, для стеганосистем прихованої передачі інформації).

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

До ЦВЗ висуваються такі вимоги [1-5]:

1. ЦВДЗ повинен легко (обчислювально) витягатися законним користувачем.

2. ЦВЗ повинен бути стійким або нестійким до навмисних і випадкових впливів. Якщо ЦВЗ використовується для підтвердження дійсності, то неприпустима зміна контейнера повинна призводити до руйнування ЦВЗ (тендітний ЦВЗ). Якщо ж ЦВЗ містить ідентифікаційний код, логотип фірми тощо, то він повинен зберігатися при максимальних перекручуваннях контейнера, що звичайно, не приводять до істотних перекручувань вихідного сигналу. Наприклад, у зображенні можуть бути відредаговані колірна гама або яскравість, в аудіозаписі – посилене звучання низьких тонів тощо. Крім того, ЦВЗ повинен бути роботоздатним стосовно афінних перетворень зображення, тобто його поворотів, масштабування. При цьому треба розрізняти стійкість самого ЦВЗ і здатність декодера правильно його виявити. Скажемо, при повороті зображення ЦВЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатки, коли ЦВЗ повинен бути стійким стосовно одних перетворень і нестійким стосовно інших. Наприклад, може бути дозволене копіювання зображення (ксерокс, сканер), але накладена заборона на внесення в нього яких-небудь змін.

3. Повинна бути можливість додавання до стега додаткового ЦВЗ. Наприклад, на DVD-диску є мітка про допустимість однократного копіювання. Після здійснення такого копіювання необхідно додати мітку про заборону подальшого копіювання. Можна було б, звичайно, видалити перший ЦВЗ і записати на його місце другий, однак це суперечить припущенню про важковіддаленістю ЦВЗ. Кращим виходом є додавання ще одного ЦВЗ, після

якого перший не буде братися до уваги. Однак наявність декількох ЦВЗ на одному повідомленні може полегшити атаку з боку зловмисника, якщо не почати спеціальних заходів.

Основні множини використання технології ЦВЗ можуть бути об'єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації та прихований зв'язок.

Популярність мультимедіа-технологій викликало множину досліджень, пов'язаних з розробкою алгоритмів ЦВЗ для використання в стандартах MP3, MPEG-4, JPEG2000, захисту DVD- дисків від копіювання.

1.1.2 Математична модель та структурна схема стеганографічної системи. Класифікація контейнерів

У загальному випадку стеганосистема може бути розглянута як система зв'язку [1]. Узагальнена структурна схема стеганосистеми наведена на рис. 1.3.

Основними стеганографічними поняттями є повідомлення і контейнер. Повідомлення $m \in M$ – це секретна інформація, наявність якої необхідно приховати, $M=\{m_1, m_2,\ldots m_n\}$ – множина всіх повідомлень.

Контейнером $c \in C$ називається несекретна інформація, яку можна використовувати для приховання повідомлення, $C=\{c_1, c_2,\ldots c_q\}$ – множина всіх контейнерів, причому $q>>n$. Як повідомлення й контейнер можуть виступати як звичайний текст, так і файли мультимедійного формату.

Порожній контейнер (або так званий контейнер-оригінал) – це контейнер c, що не містить прихованої інформації. Заповнений контейнер (контейнер-результат) – контейнер c, що містить приховану інформацію m (c_m). Одна з вимог, що при цьому висувається: контейнер-результат не повинен візуально відрізнятися від контейнера-оригіналу. Виділяють два основних типи контейнера: потоковий і фіксований.

Потоковий контейнер становить послідовність бітів, що безупинно змінюються. Повідомлення вбудовується в нього в реальному масштабі часу,

тому в кодері заздалегідь невідомо, чи вистачить розмірів контейнера для передачі усього повідомлення. В один контейнер великого розміру може бути вбудовано кілька повідомлень. Інтервали між вбудованими бітами визначаються генератором псевдовипадкової послідовності (ПВП) із рівномірним розподілом інтервалів між відліками.

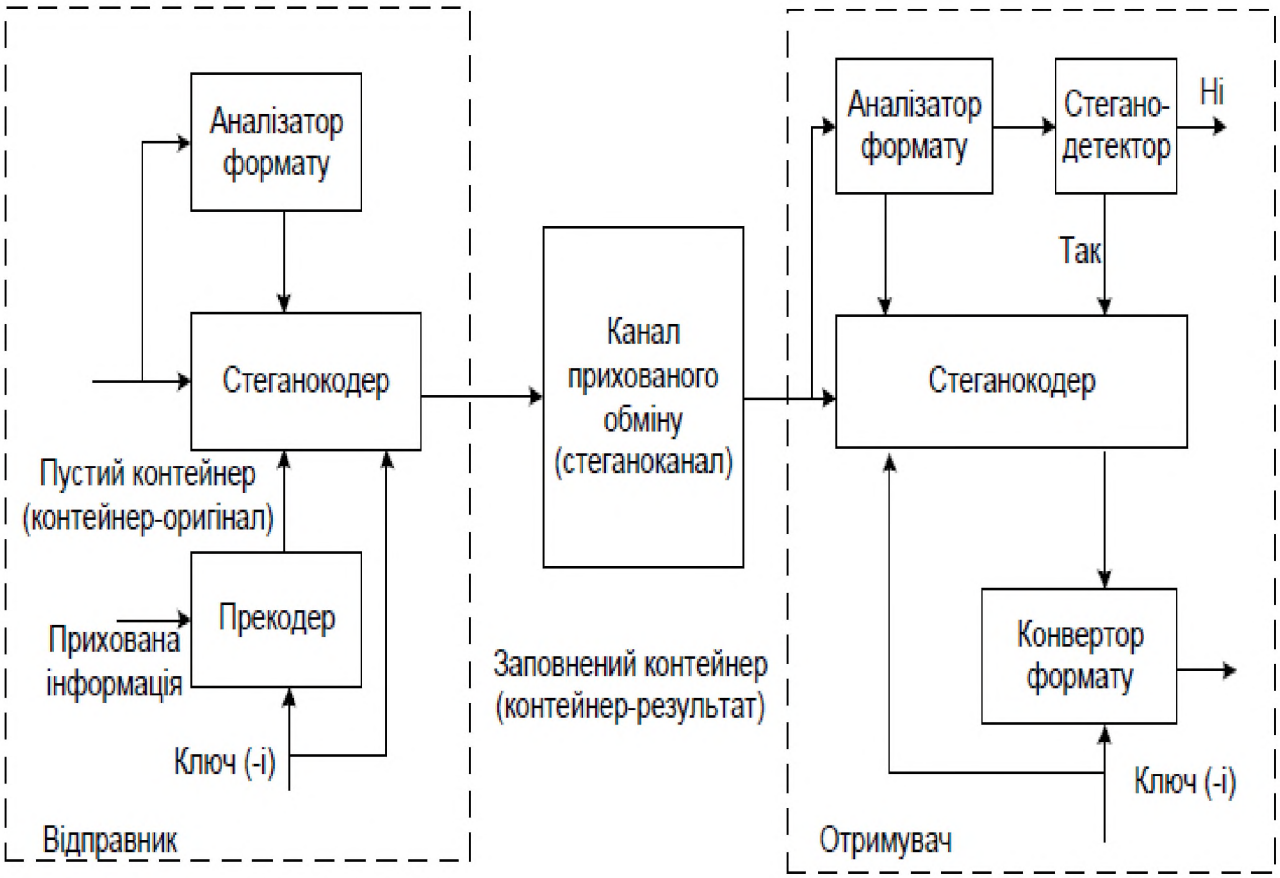

Рисунок 1.3 – Структурна схема стеганосистеми як системи зв’язку

Основна проблема полягає у виконанні синхронізації, визначенні початку та кінця послідовності. Якщо в даних контейнера існують біти синхронізації, заголовки пакетів тощо, то прихована інформація може випливати відразу ж після них. Складність організації синхронізації є перевагою з погляду забезпечення прихованості передачі. На жаль, наразі практично відсутні роботи, присвячені розробці стеганосистем із потоковим контейнером [1].

Як приклад перспективної реалізації потокового контейнера можна навести стеганоприставку до звичайного телефону. При цьому під прикриттям

пересічної, несуттєвої телефонної розмови можна передавати іншу розмову, дані тощо. Не знаючи секретного ключа, не можна не тільки довідатися про зміст прихованої передачі, але й про самий факт її існування.

У фіксованому контейнері розміри і характеристики останнього заздалегідь відомі. Це дозволяє виконувати вкладення даних оптимальним (у визначеному змісті) чином.

Контейнер може бути вибраним, випадковим або нав'язаним. Вибраний контейнер залежить від вбудованого повідомлення, а в граничному випадку є його функцією. Такий тип контейнера більше характерний саме для стеганографії. Нав'язаний контейнер з'являється, коли особа, що надає контейнер, підозрює про можливу приховану переписку і бажає їй запобігти. На практиці ж найчастіше мають справу з випадковим контейнером.

Приховання інформації, що переважно має великий обсяг, висуває істотні вимоги до контейнера, розмір якого повинен щонайменше в кілька разів перевищувати розмір даних, що вбудовуються. Зрозуміло, що для збільшення прихованості зазначене співвідношення повинне бути якомога більшим.

Перед тим як виконати вкладення повідомлення в контейнер, його необхідно перетворити в певний зручний для впакування вид. Крім того, перед впакуванням у контейнер, для підвищення захищеності секретної інформації останню можна зашифрувати досить стійким криптографічним кодом. У багатьох випадках також бажана стійкість отриманого стегоповідомлення до перекручувань (у тому числі і злочинних).

У процесі передачі звук, зображення або будь-яка інша інформація, використовувана як контейнер, може піддаватися різним трансформаціям (у тому числі з використанням алгоритмів із втратою даних): зміна обсягу, перетворення в інший формат тощо, тому для збереження цілісності вбудованого повідомлення може знадобитися використання коду з виправленням похибок (завадостійке кодування).

Початкову обробку приховуваної інформації виконує наведений на рис. 1.3 прекодер. Як одну з найважливіших попередніх обробок повідомлення (а

також і контейнера) можна назвати обчислення його узагальненого перетворення Фур'є. Це дозволяє здійснити вбудовування даних у спектральній множині, що значно підвищує їх стійкість до перекручувань.

Слід зазначити, що для збільшення таємності вбудовування попередня обробка досить часто виконується із використанням ключа.

Упакування повідомлення в контейнер (з урахуванням формату даних, що представляють контейнер) виконуються за допомогою стеганокодера. Вкладення відбувається, наприклад, шляхом модифікації найменших значущих бітів контейнера. Взагалі, саме алгоритм (стратегія) внесення елементів повідомлення у контейнер визначає методи стеганографії, які, у свою чергу, діляться на визначені групи, наприклад, залежно від того, файл якого формату був обраний як контейнер.

У більшості стеганосистем для впакування та витягнення повідомлень використовується ключ, що визначає секретний алгоритм, який визначає порядок внесення повідомлення в контейнер. За аналогією із криптографією, тип ключа спричиняє існування двох типів стеганосистем :

1. З секретним ключем – використовується один ключ, що визначається до початку обміну стеганограмою або передається захищеним каналом.

2. З відкритим ключем – для впакування та розпакування повідомлення використовуються різні ключі, які відрізняються таким чином, що за допомогою обчислень неможливо одержати один ключ із іншого, тому один із ключів (відкритий) може вільно передаватися по незахищеному каналу. Як секретний алгоритм може бути використаний генератор псевдовипадкової послідовності бітів.

Якісний генератор ПВП, орієнтований на використання в системах захисту інформації, повинен відповідати певним вимогам.

1. Криптографічна стійкість – відсутність у зловмисника можливості передбачити наступний бітів на підставі відомих йому попередніх з імовірністю, відмінною від 1/2. На практиці криптографічна стійкість оцінюється статистичними методами. Національним інститутом стандартів і

технологій США (NIST) розроблений посібник із проведення статистичних випробувань генераторів ПВП, орієнтованих на використання в задачах криптографічного захисту інформації.

2. Статистичні властивості – ПВП за своїми статистичними властивостями не повинна істотно відрізнятися від істинно випадкової послідовності.

3. Великий період формованої послідовності.

4. Ефективна апаратно-програмна реалізація. Статистично (криптографічно) безпечний генератор ПВП повинен відповідати таким вимогам: жоден статистичний тест не визначає в ПВП ніяких закономірностей, іншими словами, не відрізняє цю послідовність від істинно випадкової; при ініціалізації випадковими значеннями генератор породжує статистично незалежні псевдовипадкові послідовності.

Стеганографічний канал – канал передачі контейнера-результату (взагалі, існування каналу як, власне кажучи, і одержувача – найбільш узагальнений випадок, оскільки заповнений контейнер може, наприклад, зберігатися у «відправника», що поставив перед собою мету обмежити неавторизований доступ до певної інформації. У цьому випадку відправник виступає в ролі одержувача). Під час перебування в стеганографічному каналі контейнер, що містить приховане повідомлення, може піддаватися навмисним атакам або випадковим завадам.

У стеганодетекторі визначається наявність у контейнері (можливо вже зміненому) прихованих даних. Ця зміна може бути обумовлена впливом похибок у каналі зв'язку, операцій обробки сигналу, навмисних атак порушників. Як вже відзначалося вище, у багатьох моделях стеганосистем сигнал-контейнер розглядається як адитивний шум. Тоді завдання виявлення й виділення стеганоспілкування є класичним для теорії зв'язку.

Але слід зауважити, що такий підхід не враховує двох факторів: невипадкового характеру контейнера й вимог зі збереження його якостей. Ці моменти не зустрічаються у відомій теорії виявлення й виділення сигналів на

тлі адитивного шуму. Очевидно, що їх облік дозволить побудувати більш ефективні стеганосистеми.

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

Отже, у стеганосистемі відбувається об'єднання двох типів інформації таким чином, щоб вони по-різному сприймалися принципово різними детекторами. У якості одного з детекторів виступає система виділення прихованого повідомлення, у якості іншого – людина.

Алгоритм вбудовування повідомлення в найпростішому випадку складається із двох основних етапів:

1. Вбудовування в стеганокодері секретного повідомлення в контейнер-оригінал.

2. Виявлення (виділення) у стеганодетекторі (декодері) прихованого зашифрованого повідомлення з контейнера-результату.

Виходячи із цього, слід розглянути математичну модель стеганосистеми. Процес тривіального стеганографічного перетворення описується залежностями:

$$E: C \times M \rightarrow S, \tag{1.1}$$

$$D: S \rightarrow M, \tag{1.2}$$

де $S=\{(c_1,m_1), (c_2,m_2),\ldots,(c_n,m_n),\ldots,(c_q,m_q)\}$ – множина контейнерів-результатів (стеганограм).

Залежність (1.1) описує процес приховання інформації, залежність (1.2) – витягнення прихованої інформації. Необхідною умовою при цьому є відсутність «перетинання» [1], тобто, якщо $m_a \neq m_b$, причому $m_a \neq m_b \in M$, а $(c_a,m_a), (c_b,m_b) \in S$, то $E(c_a, m_a) \cap E(c_b, m_b) = \varnothing$.

Крім того, необхідно, щоб потужність множини $|C| \geq |M|$. При цьому обидва адресати (відправник і одержувач) повинні знати алгоритм прямого (E) і зворотного (D) стеганографічних перетворень.

Отже, у загальному випадку стеганосистема – це сукупність $\sum=(C,M,S,E,D)$ контейнерів (оригіналів і результатів), повідомлень і перетворень, які їх пов'язують.

Для більшості стеганосистем множина контейнерів C вибирається таким чином, щоб у результаті стеганографічного перетворення (1.1) заповнений контейнер і контейнер-оригінал були подібні, що формально може бути оцінене за допомогою функції подібності [1-12].

Нехай C – непуста множина, тоді функція $\mathrm{sim}(C)\rightarrow(-\infty,1)$ є функцією подоби на множині C, якщо для яких-небудь $x,y\in C$ справедливо, що $\mathrm{sim}(x,y)=1$ у випадку $x=y$ та $\mathrm{sim}(x,y)<1$ при $x\neq y$.

Стеганосистема може вважатися надійною, якщо $\mathrm{sim}[c,E(c,m)]\approx 1$ для всіх $m\in M$ і $c\in C$, причому як контейнер c повинен обиратися такий, який раніше не використовувався. Крім того, неавторизована особа не повинна мати доступ до набору контейнерів, використовуваних для секретного зв'язку.

Вибір визначеного контейнера із набору можливих контейнерів C може здійснюватися довільно (так званий сурогатний метод вибору контейнера) або шляхом обрання найбільш придатного, який менше інших зміниться під час стеганоперетворення (селективний метод). В останньому випадку контейнер обирається відповідно до правила:

$$c = \max_{x\in C} sim[x, E(x,m)]. \tag{1.3}$$

Також слід зазначити, що функції прямого (E) і зворотного (D) стеганографічних перетворень в загальному випадку можуть бути довільними (але, звичайно, відповідають одна одній), однак на практиці вимоги до стійкості прихованої інформації накладають на зазначені функції визначені обмеження.

Так, у переважній більшості випадків

$$E(c,m)\approx E(c+\delta,m), \tag{1.4}$$

$$D[E(c,m)]\approx D[E(c+\delta,m)]=m, \tag{1.5}$$

тобто незначно модифікований контейнер (на величину δ) не повинен призводити до зміни прихованої в ньому інформації.

1.1.3 Принципи стиснення зображень JPEG і JPEG 2000

Наразі більшість досліджень присвячено використанню в якості стегоконтейнера зображень [1-5]. Це обумовлено наступними причинами:

- існуванням практично важливої задачі захисту фотографій, картин, відео від незаконного тиражування і розповсюдження;

- відносно великим обсягом цифрового представлення зображень, що дозволяє впроваджувати ЦВЗ великого обсягу або підвищувати робастність впровадження;

- заздалегідь відомим розміром контейнера, відсутністю обмежень, що накладаються вимогами реального часу;

- наявністю у більшості реальних зображень текстурних областей, що мають шумову структуру і добре підходять для вбудовування інформації;

- слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів;

- добре розробленими в останнім часом методами цифрової обробки зображень.

Треба відзначити, що остання причина викликає і значні труднощі в забезпеченні робастності ЦВЗ: чим більш досконалими стають методи стиснення, тим менше залишається можливостей для вбудовування сторонньої інформації. Розвиток теорії і практики алгоритмів стиснення зображень призвело до зміни уявлень про техніку впровадження ЦВЗ. Якщо спочатку пропонувалося вкладати інформацію в незначні біти для зменшення візуальної помітності, то сучасний підхід полягає у встановленні ЦВЗ в найбільш суттєві області зображень, руйнування яких призведе до повної деградації самого зображення. Тому не випадково стегоалгоритми враховують властивості системи людського зору (СЛЗ), аналогічно алгоритмам стиску зображень. У стегоалгоритмі часто використовуються ті ж перетворення, що й в сучасних алгоритмах стиснення (дискретне косинусне перетворення в JPEG, вейвлет-

перетворення в JPEG2000 тощо). При цьому існують, очевидно, три можливості. Вкладення інформації може проводитися в початкове зображення, або одночасно із здійсненням стиснення зображення-контейнера, або в уже стисле алгоритмом зображення. Тому властивості людського зору і їх облік в алгоритмах стиснення зображень є важливими.

Найбільший інтерес в області цифрових зображень представляють методи вбудовування інформації в зображення, при використанні яких відбувається стиснення зі втратами (формати JPEG і JPEG 2000). Для таких форматів немає сенсу вбудовувати в просторову область, оскільки після певних перетворень дані будуть відрізнятися від початкових, і тому багато повідомлень, що впроваджуються, попросту неможливо витягти, й, отже, втрачається сенс системи. Для вбудовування інформації використовується область змінюваного дозволу або частотна область. Ці підходи з'явилися пізніше попереднього і продовжують розвиватися. Методи, які використовують для приховування даних частотну область, є більш стійкими до різних можливих зовнішніх впливів на зображення-контейнер. У цій групі використовуються наступні трансформації:

- дискретне косинус-перетворення (ДКП);
- дискретне вейвлет-перетворення (ДВП);
- дискретне перетворення Фур'є (ДПФ);
- перетворення Карунена-Лоєва (ПКЛ);
- сингулярне розкладання.

Ці методи використовують переваги, якими володіє представлення зображення кінцевим набором коефіцієнтів. Такі методи мають гарні характеристики робастності. Подібні перетворення можуть застосовуватись або до окремих частин зображення, або до зображення в цілому. Алгоритм ДКП є базовим в стандарті JPEG, а ДВП – в стандарті JPEG 2000. Тому для формату JPEG 2000 найбільш підходять технології вбудовування в коефіцієнти ДВП, а для формату JPEG – в коефіцієнти ДКП. При цих методах використовується скалярне або векторне квантування. Під квантуванням розуміється процес

зіставлення великої (можливо й нескінченної) множини значень з деякою кінцевою множиною чисел. Квантування знаходить застосування в алгоритмах стиснення зі втратами JPEG і JPEG 2000. Розрізняють скалярне і векторне квантування. При векторному квантуванні відбувається відображення не окремо взятого відліку, а їх сукупності (вектора). Векторне квантування ефективніше скалярного за ступенем стиснення, при цьому є більш складним.

Наразі найбільш актуальним напрямком є вбудовування в область ДВП, при якому можливо протистояти стиску зі втратами при алгоритмі JPEG 2000. Вбудовування в область ДВП найбільш доцільно застосовувати в разі активного порушника.

Формат JPEG 2000 розроблявся ще давно з метою згодом повністю замінити JPEG, але на даний момент цього не сталося. Незважаючи на те, що популярність зображень в форматі JPEG в мережі набагато вище, формат JPEG 2000 знайшов найбільш широке застосування. Основні області застосування цього формату:

• зберігання стиснутих зображень високої якості при передачі по мережі;

• цифровий кінематограф;

• 3D-візуалізація;

• охоронні системи (для стиснення зображень, одержуваних з цифрових відеокамер);

• клієнт-серверні взаємодії (бази даних зображень);

• для зберігання фотографій власника в біометричних паспортах;

• зберігання оцифрованих версій географічних карт;

• зберігання медичних файлів.

Стандарт стиснення JPEG 2000 замість ДКП, що застосовується в популярному форматі JPEG, використовує технологію ДВП, що ґрунтується на поданні сигналу у вигляді суперпозиції базових функцій – хвильових пакетів. В результаті такої компресії зображення виходить більш гладким і чітким, а розмір файлу у порівнянні з JPEG при однаковій якості виявляється набагато меншим [1-12].

Основні переваги JPEG 2000 у порівнянні із JPEG:

1. JPEG 2000 на низьких і високих бітрейтах має ступінь стиснення більше, ніж у формату JPEG. Це досягається завдяки використанню ДВП і складнішого ентропійного кодування.

2. Масштабованість фрагментів зображень. JPEG 2000 забезпечує безшовне стиснення різних компонентів зображення. Завдяки розбиттю на блоки можна зберігати зображення різних дозволів в одному кодовому потоці.

3. Довільний доступ до кодовому потоку (ROI). У форматі забезпечується декілька механізмів для підтримки довільного доступу, також підтримується декілька ступенів розбиття на частини.

4. Гнучкий формат файлу: формати файлів JP2 і JPX забезпечують зберігання інформації про кольорні простори, метаданих та інформації для узгодженого доступу в мережевих додатках, взаємодіючих за допомогою протоколу JPEG Part 9 JPIP.

ДВП пропонує велику гнучкість при поданні зображення завдяки можливості вибору коефіцієнтів перетворення для зміни різних характеристик, таких як дозвіл і якість. Найбільш цінною є можливість подання коефіцієнтів вейвлет перетворення в цілих числах, у той час як в ДКП алгоритмах робота здійснюється з коефіцієнтами, представленими у вигляді чисел з плаваючою точкою, що призводить до похибок округлення при проміжних перетвореннях, наприклад при масштабуванні. Таким чином, зміна дозволу зображення або ступеня його компресії всередині інтегрованої системи кодування, заснованої на ДВП, здійснюється без тих втрат, які були характерні для ДКП перетворень. Більш того, в ДВП є набір парних цифрових фільтрів, які можуть використовуватися для представлення зображення. За рахунок цього забезпечується можливість вибору фільтрових пар, що залежать від необхідної характеристики зображення – розміру і якості. У випадку з ДКП асоційована фільтрова система була фіксована, а для її зміни потрібно повторне кодування. Практично все програмне забезпечення наразі, яке так чи інакше стосується роботи із зображеннями, функціонує з JPEG-2000 [1-12].

Під стисненням розуміється зменшення числа біт, потрібних для цифрового представлення зображень. В основі стиснення лежать два фундаментальних явища: зменшення статистичної та психовізуальної надмірності. Можна виділити три типи статистичної надмірності [1-5]:

- просторова, або кореляція між сусідніми пікселями;
- спектральна, або кореляція між сусідніми частотними смугами;
- часова, або кореляція між сусідніми кадрами (для відео).

Високі коефіцієнти стиснення досяжні лише з використанням психовізуальної надмірності зображення, тобто нехтування його візуально незначними частинами. І тут вже не обійтися без знання системи людського зору. «Викинуті» частини зображення замінюють нулями (константами), і якщо їх багато – застосовують кодер довжин серій. У реальних алгоритмах стиснення здійснюють обнуління не пікселів зображення, а спектральних коефіцієнтів. Перевага такого підходу полягає в тому, що близькі до нуля спектральні коефіцієнти мають тенденцію розташовуватися в заздалегідь передбачуваних областях, що призводить до появи довгих серій нулів і підвищенню ефективності кодування. Великі за величиною коефіцієнти («значущі») піддають більш-менш точному квантуванню і також стискають кодером довжин серій. Останнім етапом алгоритму стиснення є застосування ентропійного кодера (Хафмана або арифметичного).

Відновлене після стиснення зображення, природно, відрізняється від початкового. За інших рівних умов, чим більше стиснення, тим більше спотворення. Для оцінки якості відновленого зображення можна використовувати міру середньоквадратичного відхилення, яке визначається як

$$СКВ = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \hat{x}_i\right)^2, \qquad (1.6)$$

де N – число пікселів в зображенні, $x_i, \hat{x}_i$ – значення пікселів початкового і відновленого зображень, відповідно.

Набагато частіше застосовується модифікація середньоквадратичного відхилення – пікове відношення сигнал / шум, яке визначається наступним чином:

$$ПВСШ = 10\log_2 \frac{N255^2}{\sum_{i=1}^{N}(x_i - x_i)^2} \quad (1.7)$$

де 255 – максимальне значення яскравості півтонування (тобто 8 біт / піксель).

Слід зазначити, що відновлене зображення вважається прийнятним, якщо $ПВСШ \geq 28-30$ дБ (у середньому). Перераховані об'єктивні заходи спотворення не завжди корелюють із суб'єктивним сприйняттям зображень, однак нічого кращого досі не придумано.

ПВСШ не завжди добре узгоджується з візуально спостережуваною похибкою. Нехай є два зображення, які повністю однакові, крім невеликої області. Хоча візуально різниця між цими зображеннями добре помітна, ПВСШ буде приблизно однаковим. Облік системи людського зору в схемі стиснення є важким завданням. Було проведено багато досліджень, але в силу труднощів з математичним описом системи зору людини більш підходящої міри знайдено не було.

Процес впровадження прихованої інформації в зображення в якомусь сенсі дуальний процесу їх стиснення [1-12]. Вбудовування інформації найчастіше здійснюють в незначущі області, щоб не змінити візуальне представлення зображення. Оптимальний метод стиснення видалить цю інформацію. На щастя, сучасні алгоритми стиснення залишають достатньо можливостей для реалізації витончених способів впровадження даних.

1.2 Вейвлети Добеші

Дискретне вейвлет перетворення здійснюється за допомогою розкладання вихідного сигналу на взаємно ортогональний набір вейвлетів, що є основною відмінністю від безперервного перетворення. Одним з перших відомих

ортогональних дискретних вейвлетів, є вейвлет Хаара. Вейвлет функція має вигляд прямокутних імпульсів – меандр. Недоліком вейвлета Хаара є те, що його базова функція добре локалізована в просторі, але погано локалізована в частотної області, оскільки меандр має широкий спектр частот [13-31].

Оскільки для повної реконструкції сигналу можуть бути застосовані тільки ортогональні вейвлети з компактним носієм, то перевагою вейвлетів сімейства Добеші перед іншими вейвлетами є те, що їх використання не вносить додаткової надмірності в вихідні дані і сигнал може бути повністю відновлений з використанням квадратурних дзеркальних фільтрів. Даний тип вейвлетів розраховується за допомогою ітераційних виразів, а форма залежить від ступеня полінома і кількості розрахованих коефіцієнтів.

Вейвлети Добеші названі на честь математика з США, яка першою побудувала дане сімейство, Інгрід Добеші (Ingrid Daubechies). Вона ввела вейвлет ψ і функцію шкали (будівельний блок) φ наступним чином. Одна вимога полягала в тому, щоб функція шкали φ мала компактний носій. Вона повинна дорівнювати нулю поза кінцевого відрізка. Добеші вибрала в якості носія відрізок [0, 3]. Вона довела, що цю функцію не можна виразити через відомі елементарні функції: многочлени, тригонометричні або ступеневі функції. Вона також показала, що φ можна побудувати рекурсивно, за допомогою деякого початкового завдання і рекурсивного правила. Вона вибрала наступні початкові значення:

$$\varphi(0)=0,\quad \varphi(1)=\frac{1+\sqrt{3}}{2},\quad \varphi(2)=\frac{1-\sqrt{3}}{2},\quad \varphi(3)=0, \tag{1.8}$$

і задала рекурсивне співвідношення

$$\varphi(r)=\frac{1+\sqrt{3}}{4}\varphi(2r)+\frac{3+\sqrt{3}}{4}\varphi(2r-1)+\frac{3-\sqrt{3}}{4}\varphi(2r-2)+\frac{1-\sqrt{3}}{4}\varphi(2r-3)=$$

$$=h_0\varphi(2r)+h_1\varphi(2r-1)+h_2\varphi(2r-2)+h_3\varphi(2r-3)=$$

$$=(h_0,h_1,h_2,h_3)\cdot(\varphi(2r),\varphi(2r-1),\varphi(2r-2),\varphi(2r-3)). \tag{1.9}$$

Подальше обчислення значень функції φ відбувається по шагам. Функція φ служить будівельним блоком для побудови вейвлета Добеші ψ, який задається також рекурсивно.

На рис. 1.4 представлені скейлінг φ(t) і вейвлет ψ(t) функції Добеші другого, третього и четвертого порядку.

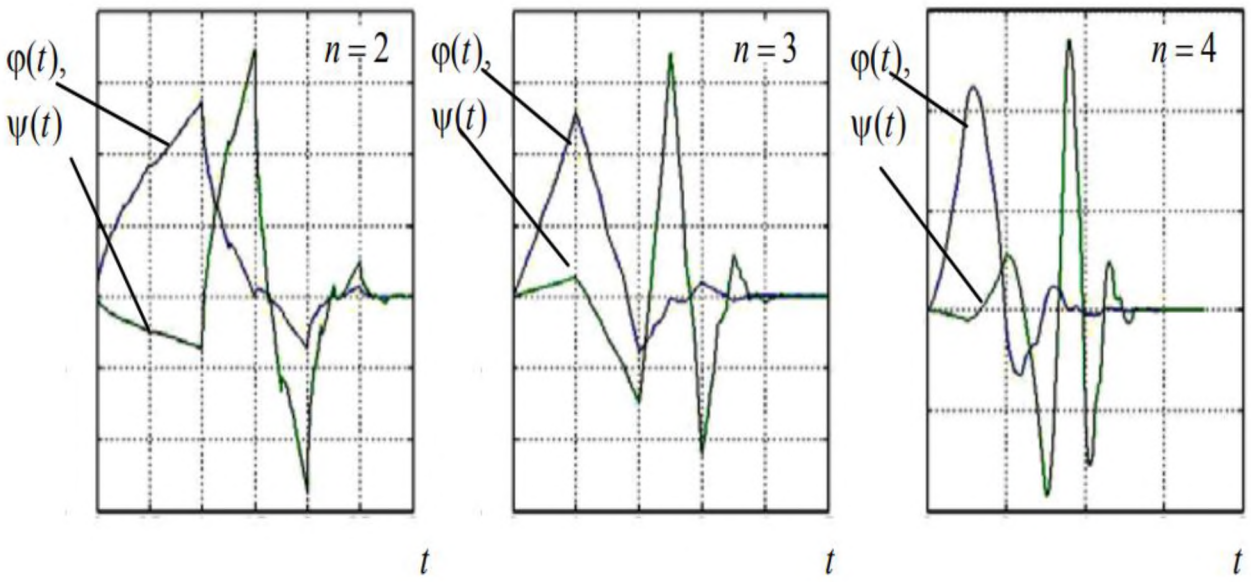

Рисунок 1.4 – Скейлінг φ(t) і вейвлет ψ(t) функції Добеші другого, третього и четвертого порядку

Очевидно, що вейвлети більш високого порядку (третього, четвертого) більш гладкі порівняно з вейвлетами другого порядку; всі функції φ_n і ψ_n несиметричні. Порядок вейвлета визначає число нульових моментів. Слід зазначити, що чим більше число нульових моментів містить вейвлет (тобто чим вище його порядок), тим більш тонку структуру сигналу він дозволяє аналізувати.

Частотно-часова характеристика фільтрів Добеші (рис. 1.5) дає можливість з найбільшою ймовірністю виявити локальний сигнал, ґрунтуючись на частотному діапазоні самого локального сигналу і діапазоні на який налаштований фільтр (при наявності базових апріорних знань про вхідний сигнал). Виробляючи вибір відповідного кроку дискретизації сигналу можна

забезпечити максимальний відгук вейвлет коефіцієнтів при перетворенні. Це є основоположною задачею при виділенні ЛС з сильно зашумленого вимірювального каналу.

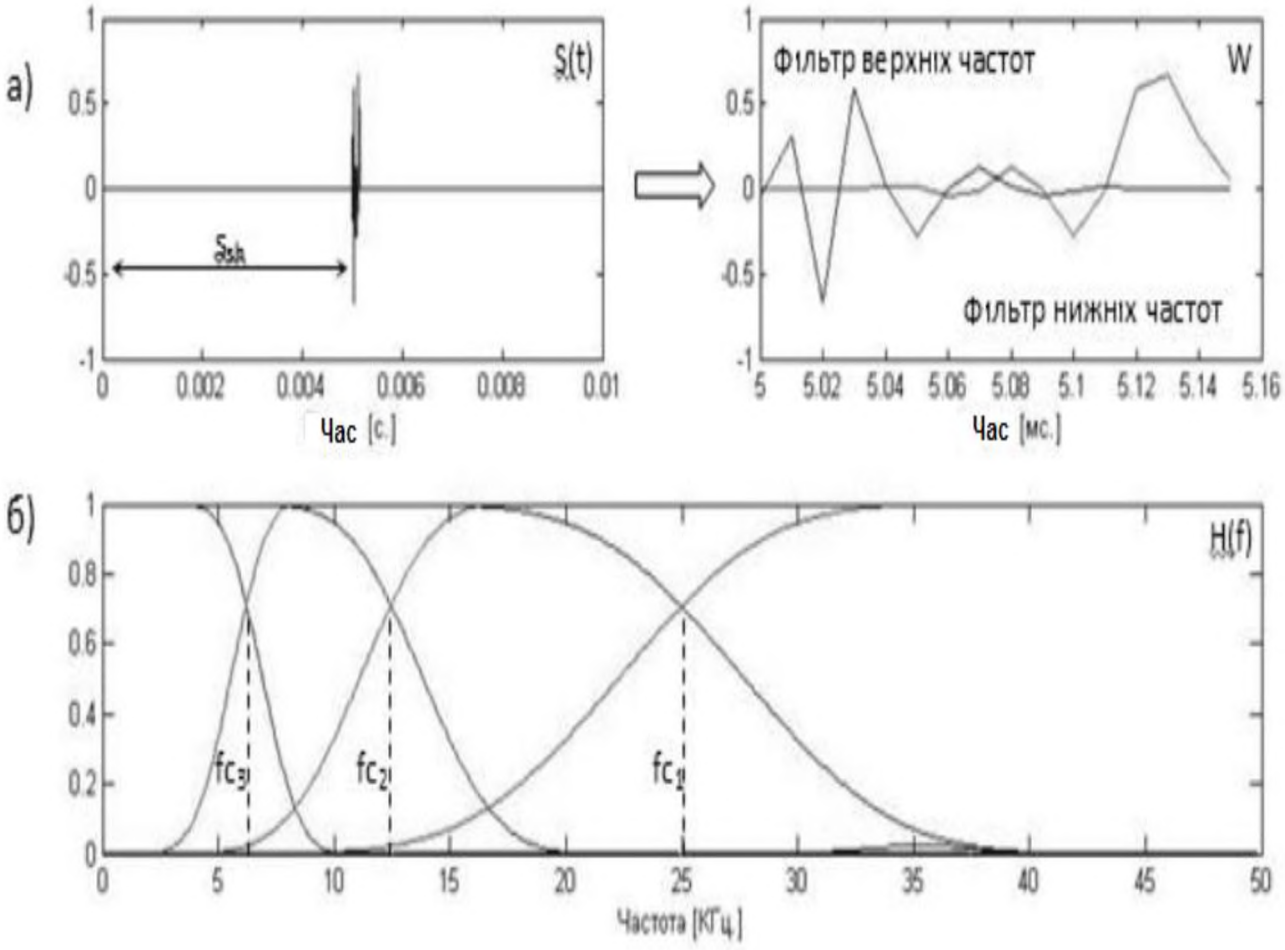

Рисунок 1.5 – Зображення часової (*а*) і частотної (*б*) характеристик вейвлет фільтрів Добеші

Кожному рівню вейвлет-розкладання ЛС, характерна своя частота зрізу f_c – значення частоти, при якому відбувається розподіл вейвлет коефіцієнтів на апроксимуючі (низькочастотні) і деталізуючі (високочастотні). У цей момент відбувається спад амплітуди вихідного сигналу до значення 0,7 від значення в смузі пропускання фільтра.

На побудованій амплітудно-частотній характеристиці (рисунок 1.5,*б*) відзначені значення частот зрізу (f_{c1}, f_{c2}, f_{c3}) для кожного з рівнів вейвлет розкладу j.

Основні властивості вейвлетів сімейства Добеші:

- мають хороший локалізований спектр в частотної області, характеризуються двома функціями: вейвлет функцією ψ і масштабуючою функцією φ;

- є вейвлетами ортогонального типу, зосереджені на кінцевому інтервалі часу і мають кінцеве кількість фільтруючих коефіцієнтів;

- здатні повністю відновити довільний локальний сигнал на нульовому рівні реконструкції;

- мають можливість виконувати дискретні перетворення з застосуванням алгоритмів швидкого вейвлет перетворення (ШВП).

Слід зазначити, що наразі найвідомішим з існуючих вейвлетних перетворень є вейвлетне перетворення Добеші 9/7. Крім того, воно вважається й одним з найбільш ефективних. Зайвим доказом цього може бути те, що перетворення Добеші 9/7 було вибрано за основу в стандарті для стиснення зображень JPEG2000 [11, 13-31].

1.3 Існуючі підходи до вбудовування додаткової інформації у цифрові зображення

Відомий підхід до впровадження додаткової інформації в цифрові зображення «Захист від статистичного стегоаналізу», в якому для протидії деяким методам аналізу при запису інформації використовується тільки частина молодших значущих бітів в байтах колірного представлення початкового зображення. А біти, які залишились, використовуються для подальшої корекції найбільш важливих статистичних параметрів [32].

Відомий також підхід до впровадження додаткової інформації в цифрові зображення [33], що полягає в тому, що початкове цифрове зображення розкладають на бітові шари, для запису додаткової інформації вибирають один з отриманих бітових шарів, який представляють як бітову послідовність, запис додаткової інформації здійснюють за допомогою коду. При цьому в отриманій

бітовій послідовності біти, розташовані на кордонах усіх переходів однакових послідовностей нулів і одиниць, замінюють відповідно до бітів записуваної додаткової інформації. А біти, які залишились та що відносяться до нижчих бітових шарів при необхідності використовують для корекції початкового зображення або для запису іншої додаткової інформації.

Завданням, на вирішення якої спрямовано відомий підхід до впровадження додаткової інформації в цифрові зображення [33], є підвищення рівня захисту конфіденційної інформації при її прихованому зберіганні і передачі по відкритих каналах зв'язку, в разі використання в якості контейнерів растрових фотореалістичних зображень, а також підвищення відносного обсягу інформації, що приховується за рахунок використання середніх і старших розрядів інформаційних байтів зображення.

Вищевказане досягається за рахунок того, що для впровадження інформації вибираються ті біти початкового зображення, поведінка яких найменш передбачувана і зміна яких не призведе до помітних спотворень початкового зображення. В якості таких бітів кодером вибираються біти, розташовані на кордонах між різними областями зображення, при цьому пошук відповідних бітів в зображенні здійснюється автоматично безпосередньо під час запису додаткової інформації. З оброблюваного зображення виділяється бітова послідовність, яка подається на вхід кодера або декодера, при цьому запис або вилучення інформації здійснюється тільки в тих випадках, коли в вікно перегляду кодера або декодера потрапляє ділянка бітової послідовності, що містить перехід від 0 до 1 або від 1 до 0 . В процесі впровадження інформації зміни можуть бути піддані як біти, що належать обраній бітовій послідовності, так і біти, що залишились. При цьому частина бітів може використовуватись для компенсації внесених спотворень як в процесі запису інформації, так і при подальшій корекції отриманого зображення.

Технічним результатом застосування відомого підходу до впровадження додаткової інформації в цифрові зображення [33] є підвищення обсягів впроваджуваної інформації за рахунок використання як молодших, так і

старших значущих бітів байтів колірного представлення точок зображення, при достатньому збереженні візуальної якості зображення. Останнє можливо завдяки тому, що в фотореалістичних зображеннях поведінку точок, розташованих на кордоні між різними областями зображення, отриманого за допомогою цифрового перетворення, залежить від великого числа випадкових чинників і складно передбачувано. Використання спеціального коду, у свою чергу, дозволяє зберегти більшість статистичних параметрів зображення з досить високою точністю і звести до мінімуму число додатково контрольованих параметрів і коригувальних змін, завдяки чому вдається успішно протистояти ряду статистичних методів аналізу. Крім того, факт наявності сторонньої інформації не вдається встановити і при проведенні візуального аналізу бітових зрізів отриманого зображення.

Суть відомого підходу до впровадження додаткової інформації в цифрові зображення [33] пояснюється на прикладі обробки кодером і декодером послідовності бітів початкового зображення (рис. 1.6), отриманої відповідно до схеми на рис. 1.6.

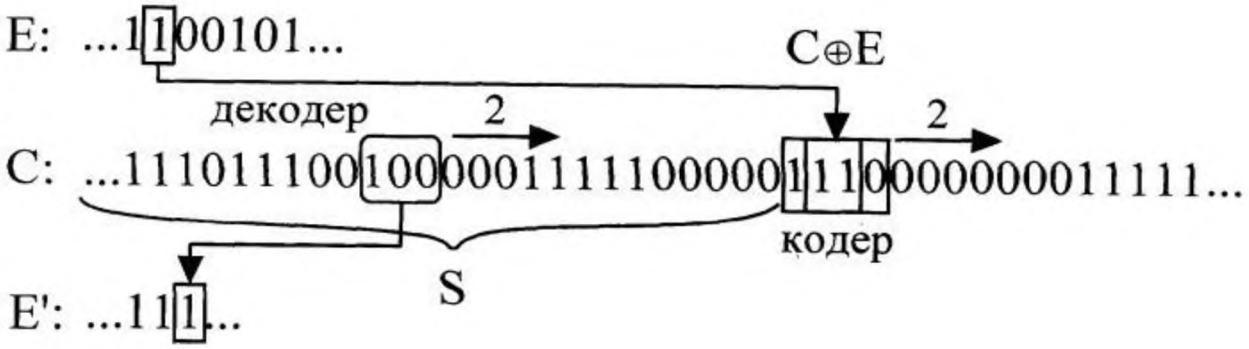

Рисунок 1.6 – Приклад обробки послідовності бітів зображення кодером і декодером, що здійснюється у рамках відомого підходу до впровадження додаткової інформації в цифрові зображення [33]

Формування бітової послідовності здійснюється згідно зі схемою послідовної обробки зображень, яка наведена на рис. 1.6.

Рисунок 1.7 – Порядок отримання бітової послідовності з кольорового зображення, представленого в цифровому вигляді згідно відомого підходу до впровадження додаткової інформації в цифрові зображення [33]

У відомому підході до впровадження додаткової інформації в цифрові зображення [33] зазначається, що для забезпечення найбільшої стійкості

інформаційна бітова послідовність повинна мати рівномірний розподіл. Найбільш ефективним є використання цього підходу до приховування інформації спільно з алгоритмами стиснення і блочного шифрування застосовуються послідовно до приховуваного повідомленням.

Відомий також підхід до вбудовування повідомлення в цифрове зображення [34], що полягає в заміні найменш значущого біта в байтах початкового цифрового зображення. При цьому найменш значущому біту в байтах початкового цифрового зображення присвоюють флагове значення «одиниця» при співпадінні частини бітів байту сигналу цифрового зображення і бітів сигналу повідомлення, або флагове значення «нуль» при розбіжності. При цьому коригування статистики розподілу найменш значущих бітів здійснюють по їх частини, що залишилась, і яка не використовується в якості флагових значень.

Пристрій, що реалізовує відомий підхід до вбудовування повідомлення в цифрове зображення [34], загальна схема якого представлена на рис. 1.8 працює наступним чином.

Сигнал цифрового зображення (контейнер) 1 послідовно побітно подають на вхід блоку 2 – послідовно-паралельний перетворювач, що складається з 8-розрядного регістра зсуву і 8-розрядного буферного регістра (рис. 1.8). Тактові імпульси Т1 подають на вхід блоку 2 і на вхід блоку 5 – блок керування, що включає два 4-розрядних двійкових синхронних лічильника, два D-тригера, чотири елементи 2І-НЕ і чотири елементи 2І. Сигнал повідомлення подають послідовно побітно на вхід блоку 4 – блок зберігання вбудованих бітів повідомлення, що складається з 8-розрядного регістра зсуву.

З приходом 8-го тактового імпульсу в блоці 2 (вихід 8-розрядного регістра зсуву) формують сигнал контейнера, а на виході блоку керування (вихід Q4 4-розрядного двійкового синхронного лічильника) формують сигнал, що дозволяє передачу сигналу контейнера в паралельному вигляді на вихід блоку 2 (вихід 8-розрядного буферного регістра) і на вхід блоку 7 – блок зберігання байта сигналу стегоконтейнера – 8-розрядний буферний регістр

(рис. 1.8). З виходу блоку 4 на вхід блоку 6 (блок порівняння, що включає 4 елементи 2 АБО – компаратор, 4 елементи 2 АБО-НЕ) подають два біта вбудованого повідомлення, які порівнюють з 6 і 7 (за номером від 1 до 8) бітами відповідно сигналу контейнера, сформованого на виході блоку 2.

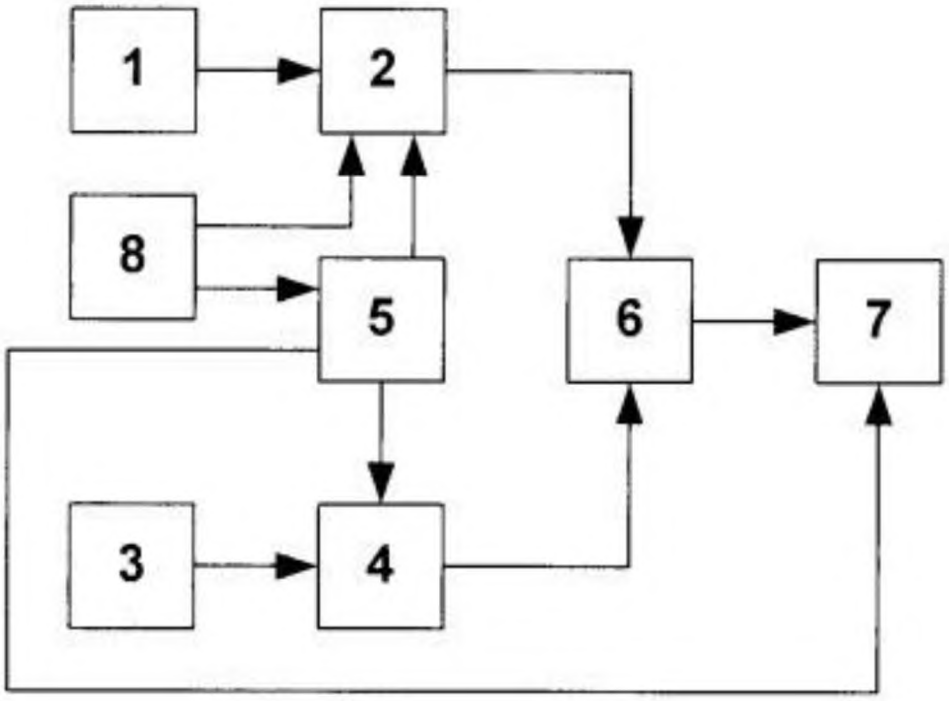

Рисунок 1.8 – Загальна схема пристрою, що реалізує відомий підхід до вбудовування повідомлення в цифрове зображення [34]

Слід підкреслити, що при попарному збізі бітів сигналу контейнера і бітів сигналу вбудованого повідомлення восьмий біт сигналу контейнера в блоці 7 встановлюють в стан логічної одиниці. Зчитування байта сигналу стегоконтейнера зі входу на вихід блоку 7 здійснюють по задньому фронту 8-го тактового імпульсу. Одночасно з цим обнулюють 4-розрядний двійковий синхронний лічильник блоку 5.

У разі встановлення восьмого біта сигналу контейнера в блоці 7 в стан логічної одиниці формують сигнал на зчитування двох чергових бітів сигналу вбудованого повідомлення в блоці 4 (рис. 1.8). Сигнал, що дозволяє зчитування чергових бітів сигналу вбудованого повідомлення, формують в блоці 5 (D-

тригер і елемент 2І) на виході Q2 лічильника через два тактових імпульси формують сигнал установки в нуль D-тригера і процес зчитування припиняють для чергового порівняння.

У разі встановлення восьмого біта сигналу контейнера в блоці 7 в стан логічного нуля (попарна розбіжність бітів сигналів контейнера і вбудованого повідомлення) зчитування байта сигналу стегоконтейнера зі входу на вихід блоку 7 також здійснюють по задньому фронту 8-го тактового імпульсу (рис. 1.8). Одночасно з цим обнулюють 4-розрядний двійковий синхронний лічильник блоку 5. Однак сигнал, що дозволяє зчитування чергових бітів сигналу вбудованого повідомлення в блоці 5 (D-тригер і елемент 2І), не формують і порівняння бітів сигналу чергового байта контейнера здійснюють із раніше записаними бітами сигналу вбудованого повідомлення.

Вилучення повідомлення, вбудованого в цифрове зображення згідно відомого підходу до вбудовування повідомлення в цифрове зображення [34] здійснюють відповідно до схеми, представленої на рис. 1.9, у наступному порядку.

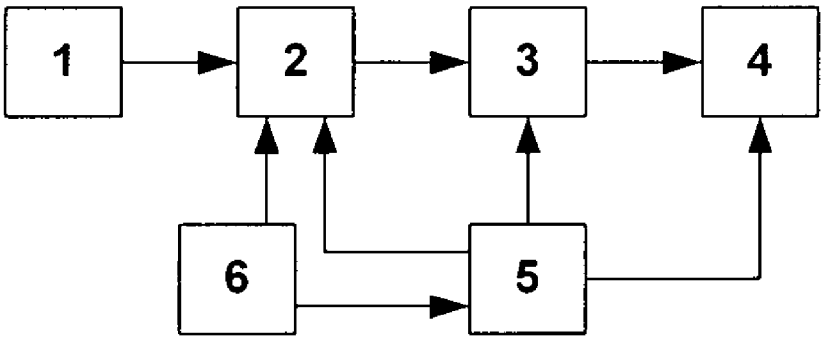

Рисунок 1.9 – Загальна схема пристрою, що реалізує вилучення повідомлення згідно відомого підходу до вбудовування повідомлення в цифрове зображення [34]

Сигнал цифрового зображення з вбудованим повідомленням (стегоконтейнер) (блок 1) послідовно побітно подають на вхід блоку 2 – послідовно-паралельний перетворювач (рис. 1.9). Тактові імпульси з блоку 6 –

генератор тактових імпульсів подають на вхід блоку 2 і на вхід блоку 5 – блок керування.

З приходом 8-го тактового імпульсу в блоці 2 формують сигнал стегоконтейнера, а на виході блоку 5 формують сигнал, що дозволяє передачу сигналу стегоконтейнера в паралельному вигляді на вихід блоку 2 (рис. 1.9).

Восьмий біт сформованого байта сигналу стегоконтейнера подають на вхід блоку 5, де виробляють його порівняння з логічною одиницею і в разі збігу формують сигнал, що дозволяє зчитування 6 і 7 (за номером від 1 до 8) бітів сигналу стегоконтейнера, що надходять на вхід блоку 3 – блок вилучення та зберігання вбудованого повідомлення (рис. 1.9).

Слід зауважити, що коригування статистики при необхідності проводять по невживаних восьмим бітам байтів стегоконтейнера.

У відомому підході до вбудовування повідомлення в цифрове зображення [34] зазначається, що для забезпечення найбільшої ефективності вбудовування в цифрове зображення повідомлення, останньому надається характер псевдовипадкової послідовності. Також підкреслюється, що найбільш ефективним є використання відомого підходу до вбудовування інформації в цифрове зображення [34] спільно з алгоритмами скремблювання і ефективного кодування.

До недоліків усіх трьох зазначених вище підходів до впровадження інформації в цифрові зображення [32-34] слід віднести неможливість їх застосування для графічних зображень стислих форматів, зокрема JPEG і JPEG 2000. В основі даних форматів лежать алгоритми стиснення зі втратами, які в свою чергу мають деградуючий вплив на впроваджувану інформацію.

Найбільш близьким за технічною сутністю до запропонованого підходу (прототипом) є підхід до створення водяних знаків для цифрових зображень і відео [35], що полягає у наступному. До початкового цифрового зображення застосовують дискретне вейвлет-перетворення, для вбудовування цифрового водяного знака вибирають вейвлет-коефіцієнти з великими значеннями в середньочастотних і в високочастотних піддіапазонах, а перед вбудовуванням

цифровий водяний знак перетворюють в псевдовипадкову послідовність. При цьому вбудовування здійснюють додаванням псевдовипадкової послідовності до обраних вейвлет-коефіцієнтів, далі до цифрового зображення застосовують зворотне дискретне вейвлет-перетворення.

Зображення може бути розкладено на пірамідну структуру, як показано на рис. 1.10, а також забезпечити різну інформацію діапазону, наприклад, низьку-низьку (LL), низьку-високу (LH), і високу-високу (HH) смуги частот. Приклад такого розкладання із двома рівнями показаний на рис. 1.11, де краї з'являються у всіх смугах, за винятком найнижчої смуги частот, тобто кутовій частині ліворуч і зверху.

Звичайні методи водяних знаків мають декілька обмежень, щодо яких даний винахід прагне вдосконалити. Наприклад, сучасні методи водяних знаків для цифрових зображень та відео, такі як підхід, заснований на ДКП, не дуже надійні, не ієрархічні за структурою, а також їх використання призводить до великих навантажень на комп'ютер для спотворених зображень. Відомий підхід до створення водяних знаків для цифрових зображень і відео [35] вирішує ці проблеми.

Водяний знак у домені ДВП включає дві частини: кодування та декодування. У частині кодування зображення спочатку розкладається на кілька смуг із пірамідною структурою, як показано на рис. 1.10 і 1.11, а потім псевдовипадкові послідовності (наприклад, гаусів шум) додаються до великих коефіцієнтів, розташованих у високих і середніх смугах частоти ДВП, тобто до великих коефіцієнтів, які не розташовані з найнижчою роздільною здатністю, наприклад, у верхньому лівому куті. Математичний аналіз частини кодування дозволяє y[m, n] позначати коефіцієнти ДВП, які не розташовані в найнижчій смузі частот зображення x[n, m]. Гаусів шум N[m, n] додається із середнім значенням 0 та дисперсією від 1 до y[m, n]. В результаті отримують наступне рівняння:

$$\bar{y}[m,n]=y[m,n]+\alpha(y[m,n])^2 N[m,n], \qquad (1.10)$$

де α – параметр для управління рівнем водяного знака, а квадрат y[m, n] вказує на посилення великих коефіцієнтів ДВП. Коефіцієнти ДВП при найнижчій роздільній здатності не змінюються.

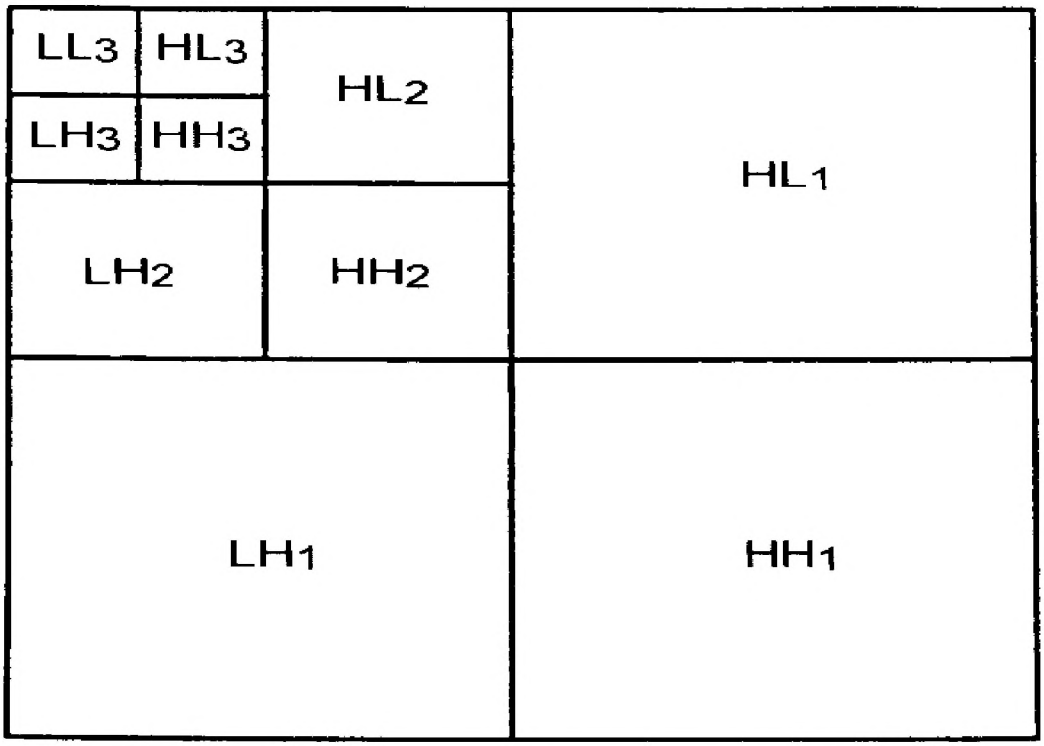

Рисунок 1.10 – Класичний варіант піраміди розкладання ДВП зображення

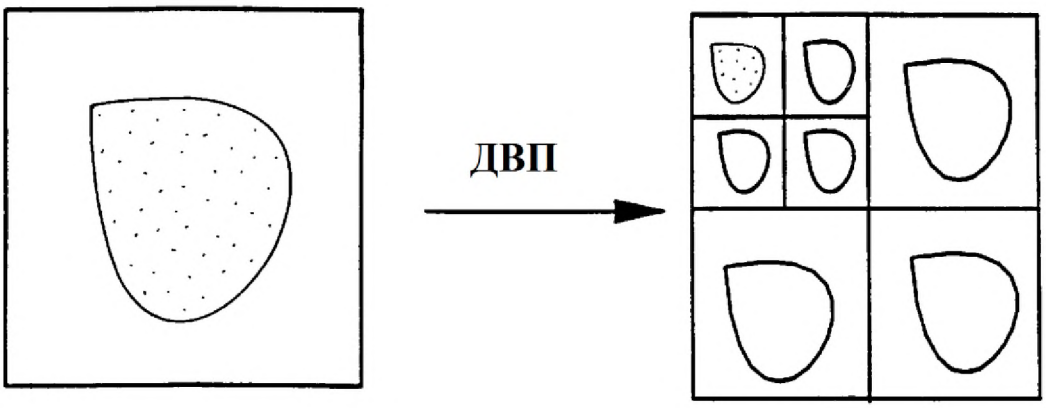

Рисунок 1.11 – Варіант піраміди розкладання зображення ДВП, із двома рівнями діапазону

Далі здійснюють двовимірне зворотне ДВП модифікованих коефіцієнтів DWT $\bar{y}$ та незмінені коефіцієнти ДВП при найнижчій роздільній здатності і

нехай $\bar{I}$ [m, n] позначає коефіцієнти зворотного ДВП. Щоб отримане зображення вмістилося в межах від 0 до 255 цілих значень, що є типовими для зображень, воно модифікується наступним чином:

$$\hat{x}[m, n] = \left[255 \frac{\tilde{x}[m, n] - \min_{m,n} (\tilde{x}[m, n])}{\max_{m,n} (\tilde{x}[m, n] - \min_{m,n} (\tilde{x}[m, n]))}\right]. \quad (1.11)$$

Операція рівняння (1.11) перетворює двовимірні дані $\bar{I}$ [m, n] у 8-бітове зображення. Отримане зображення $\bar{I}$ [m, n] – це зображення із водяним знаком x[m, n]. Процедура кодування, що здійснюється згідно відомого підходу до створення водяних знаків для цифрових зображень і відео [35] показана на рис. 1.12.

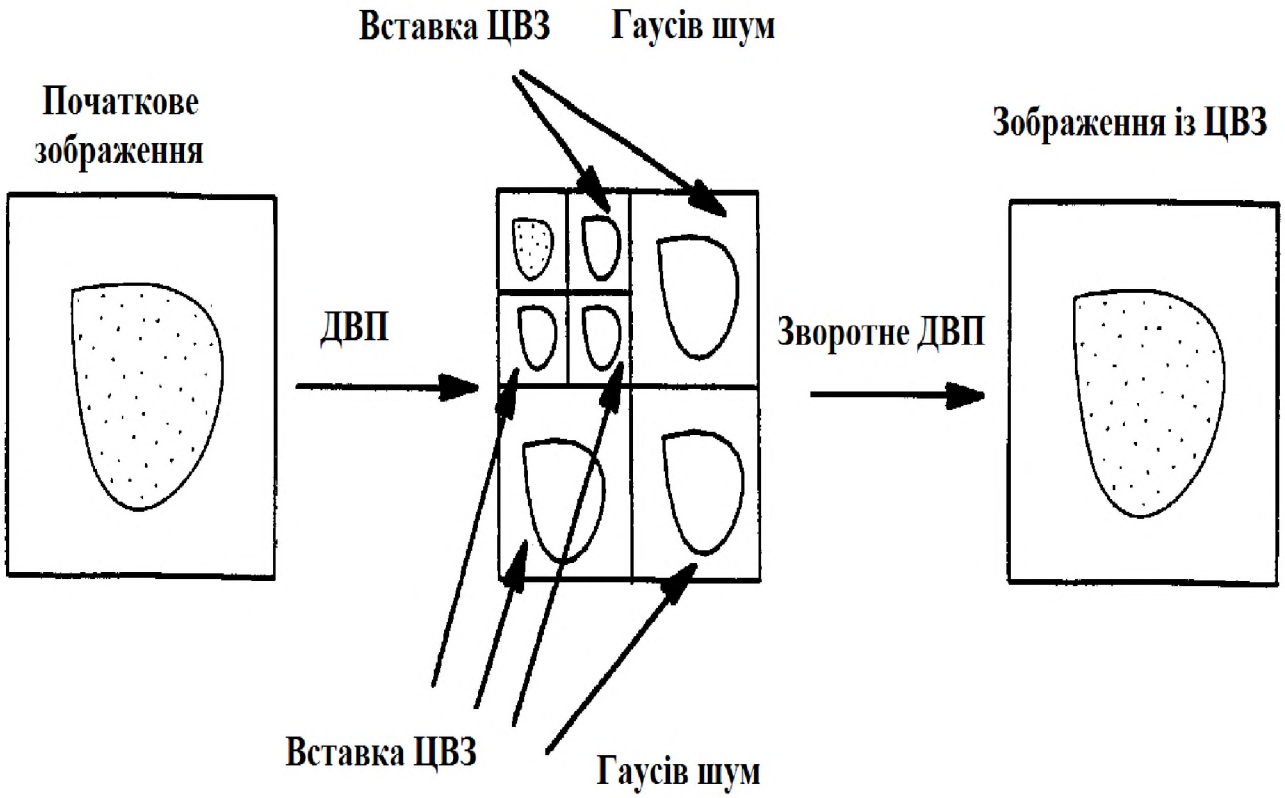

Рисунок 1.12 – Процедура кодування, що здійснюється згідно відомого підходу до створення водяних знаків для цифрових зображень і відео [35]

Процедура декодування, що здійснюється згідно відомого підходу до створення водяних знаків для цифрових зображень і відео [35] показана на рис. 1.13.

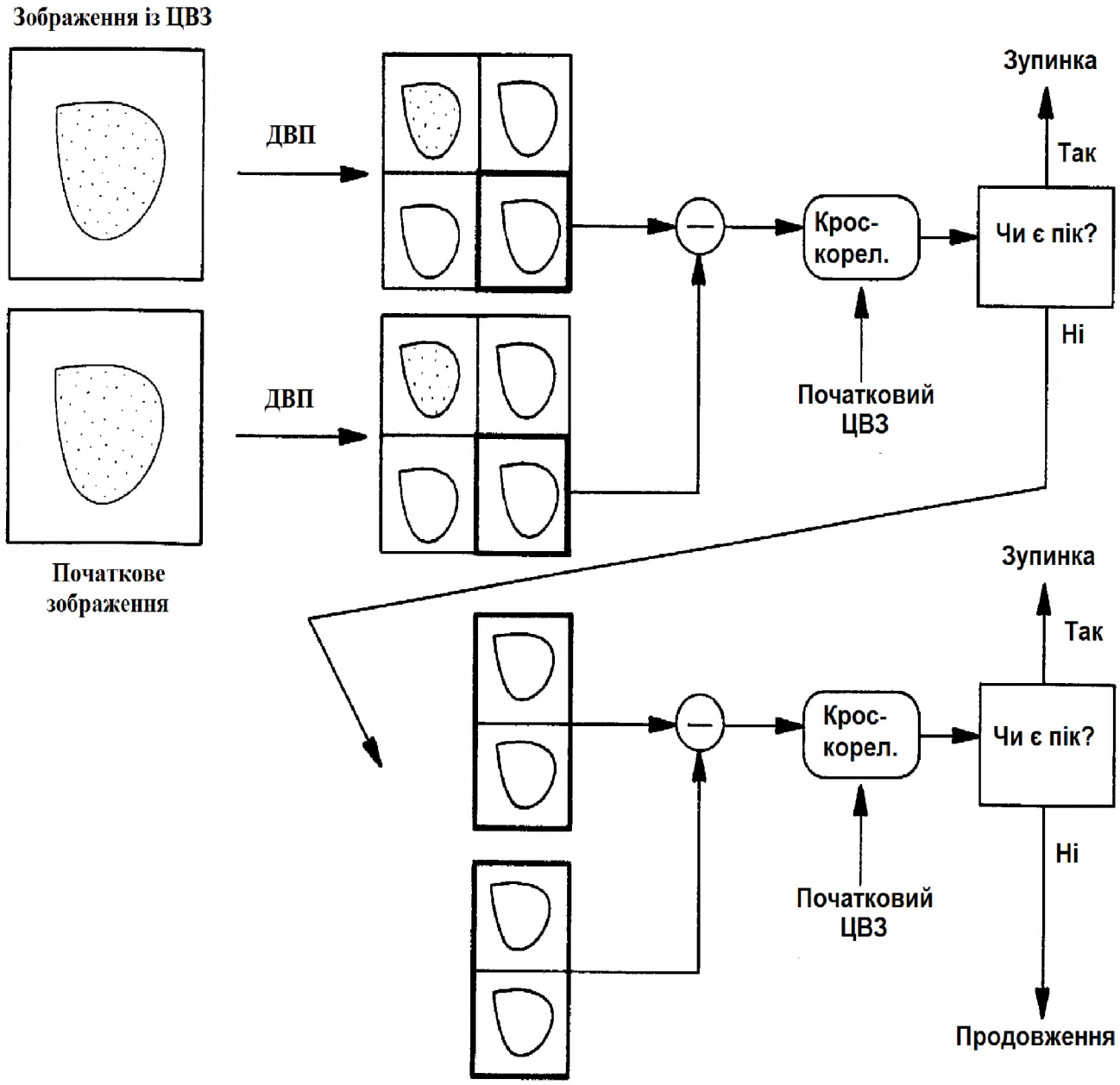

Рисунок 1.13 – Процедура декодування, що здійснюється згідно відомого підходу до створення водяних знаків для цифрових зображень і відео [35]

Процедура декодування, що здійснюється згідно відомого підходу до створення водяних знаків для цифрових зображень і відео [35] є ієрархічною і описується наступним чином. Спочатку отримане зображення та початкове

(оригінальне) зображення (передбачається, що початкове зображення відоме) розкладаються за допомогою ДВП на чотири смуги, наприклад, низька-низька (LL_1) смуга, низька-висока (LH_1) смуга, висока-низька смуга (HL_1) та висока-висока (HH_1) смуга відповідно.

Далі підпис, доданий в смузі HH_1, і різниця коефіцієнтів ДВП в смугах HH_1 прийнятого та початкового зображень порівнюються шляхом обчислення їх крос-кореляцій (або взаємних кореляцій). Якщо в крос-кореляціях є пік, визначається, що ЦВЗ виявляється. В іншому випадку ЦВЗ, доданий у смугах HH_1 та LH_1, порівнюється з різницею коефіцієнтів ДВП у смугах HH_1 та LH_1 відповідно. Якщо є пік, ЦВЗ виявляється. В іншому випадку розглядається підпис, доданий у смугах HL_1, LH_1 та HH_1. Якщо в перехресних кореляціях все ще немає піку, продовжують розкладати початковий і отримані сигнали в смузі LL_1 на чотири додаткові піддіапазони, LL_2, HL_2, LH_2 і HH_2, і так далі, поки в перехресних кореляціях не з'явиться пік . Якщо численні спроби (наприклад, 6 разів) розділити сигнали на піддіапазони не дають піку, тоді ЦВЗ визначається невизначуваним.

Слід зазначити, що недоліками відомого підходу до створення водяних знаків для цифрових зображень і відео [35] є наступні:

• часткова втрата інформації, що вбудовується, при стисненні за стандартом JPEG 2000 під час процедури квантування;

• обмежений обсяг вбудованого повідомлення внаслідок обмеженої кількості вейвлет-коефіцієнтів з великими значеннями в середньочастотних і в високочастотних піддіапазонах області вейвлет-перетворення.

1.4 Висновок. Постановка задачі

В розділі проаналізовано принципи впровадження інформації у нерухомі зображеннях, а також вейвлет-перетворень. Встановлено, що серед методів приховування найпоширенішими наразі є методи на основі вейвлет-перетворення. Ці методи є популярними, оскільки не вносять значних

спотворень у зображення, мають достатню пропускну здатність та є стійкими до навмисних атак та викривлень у каналах зв'язку.

В розділі проаналізовано існуючі підходи до вбудовування додаткової інформації у цифрові зображення. Встановлено, що недоліком відомих підходів до впровадження інформації в цифрові зображення [32-34] є неможливість їх застосування для графічних зображень стислих форматів, зокрема JPEG і JPEG 2000. В основі даних форматів лежать алгоритми стиснення зі втратами, які у свою чергу мають деградуючий вплив на впроваджувану інформацію.

Встановлено, що недоліком відомого підходу до створення водяних знаків для цифрових зображень і відео [35] є часткова втрата інформації, що вбудовується, при стисненні за стандартом JPEG 2000 під час процедури квантування, а також обмежений обсяг вбудованого повідомлення внаслідок обмеженої кількості вейвлет-коефіцієнтів з великими значеннями в середньочастотних і в високочастотних піддіапазонах області вейвлет-перетворення.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації

Запропонований підхід відноситься до області стеганографії, а саме до способів вбудовування повідомлення в цифрові зображення. Технічний результат полягає в забезпеченні можливості збереження цілісності впровадженої інформації. Запропонований підхід до вбудовування повідомлення в цифрове зображення формату JPEG 2000 полягає в заміні кодуючих коефіцієнтів средньочастотних і високочастотних піддіапазонів вейвлет-перетворення, причому вбудовування здійснюють після процедури квантування в блоки вейвлет-коефіцієнтів розміром $N \times N$, причому значення бітів вбудованого повідомлення кодують парністю суми значень вейвлет-коефіцієнтів в блоці. При цьому, якщо значення вбудованого біта не збігається з парністю суми значень вейвлет-коефіцієнтів в блоці, значення одного з них збільшують на одиницю, причому для модифікації вибирають вейвлет-коефіцієнт, значення якого має найбільшу дробову частину.

Завданням запропонованого підходу є таке вбудовування повідомлення в цифрове зображення формату JPEG 2000, яке забезпечує можливість збереження цілісності впровадженої інформації при передачі останньої по відкритих каналах зв'язку. Запропонований підхід заснований на кодуванні бітів вбудованого повідомлення сумою значень вейвлет-коефіцієнтів в блоці розміром $N \times N$ з області средньочастотних і високочастотних піддіапазонів вейвлет-перетворення. При цьому вибір розміру блоку залежить від вимог, що пред'являються до стеганосистеми: а саме, чим більше розмір блоку, тим вище стійкість стеганосистеми.

Дане завдання вирішується тим, що спосіб вбудовування повідомлення в цифрове зображення формату JPEG 2000 здійснюють після процедури

квантування в блоки вейвлет-коефіцієнтів розміром N×N, причому значення бітів вбудованого повідомлення кодують парністю суми значень вейвлет-коефіцієнтів в блоці. При цьому, якщо значення вбудованого біта не збігається з парністю суми значень вейвлет-коефіцієнтів в блоці, значення одного з них збільшують на одиницю, причому для модифікації вибирають вейвлет-коефіцієнт, значення якого має найбільшу дробову частину.

Даний вибір обумовлений тим, що в стандарті JPEG 2000 округлення квантованого коефіцієнта здійснюють до найменшого цілого

$$q_b(u, v) = \operatorname{sign}(a_b(u, v)) \times \left\lfloor \frac{|a_b(u, v)|}{\Delta_b} \right\rfloor, \tag{2.1}$$

де $q_b(u,v)$ – значення вейвлет-коефіцієнта з піддіапазона b після процедури квантування; sign – функція, яка визначає знак вейвлет-коефіцієнта, що квантується, $a_b(u,v)$ – значення вейвлет-коефіцієнта, що квантується, з піддіапазону b, Δb – крок квантування для піддіапазону b.

В результаті округлення виникає шум квантування, який тим більше, чим більше дробова частина значення коефіцієнта.

Завдяки новій сукупності суттєвих ознак в запропонованому підході реалізована можливість вбудовування конфіденційної інформації із різним ступенем стійкості до стеганоаналізу при відсутності необхідності в зміні статистичних характеристик розподілу вейвлет-коефіцієнтів.

Загальна схема пристрою, що реалізує запропонований підхід до вбудовування повідомлення в цифрове зображення формату JPEG 2000 показана на рис. 2.1.

На рис. 2.1 введено такі позначення:

1 – цифрове зображення (контейнер);

2 – генератор тактових імпульсів;

3 – пристрій зберігання повідомлення;

4 – квантувач;

5 – пристрій для реалізації дискретного вейвлет-перетворення;

6 – генератор псевдовипадкової послідовності (стеганоключ);

7 – пристрій нормування;

8 – суматор;

9 – пристрій для визначення парності;

10 – пристрій порівняння;

11 – стисле цифрове зображення із вбудованим повідомленням (стеганоконтейнер);

12 – пристрій для реалізації арифметичного кодування;

13 – комутатор;

14 – реверсивний лічильник;

15 – блок вибору вейвлет-коефіцієнта з найбільшою дробовою частиною.

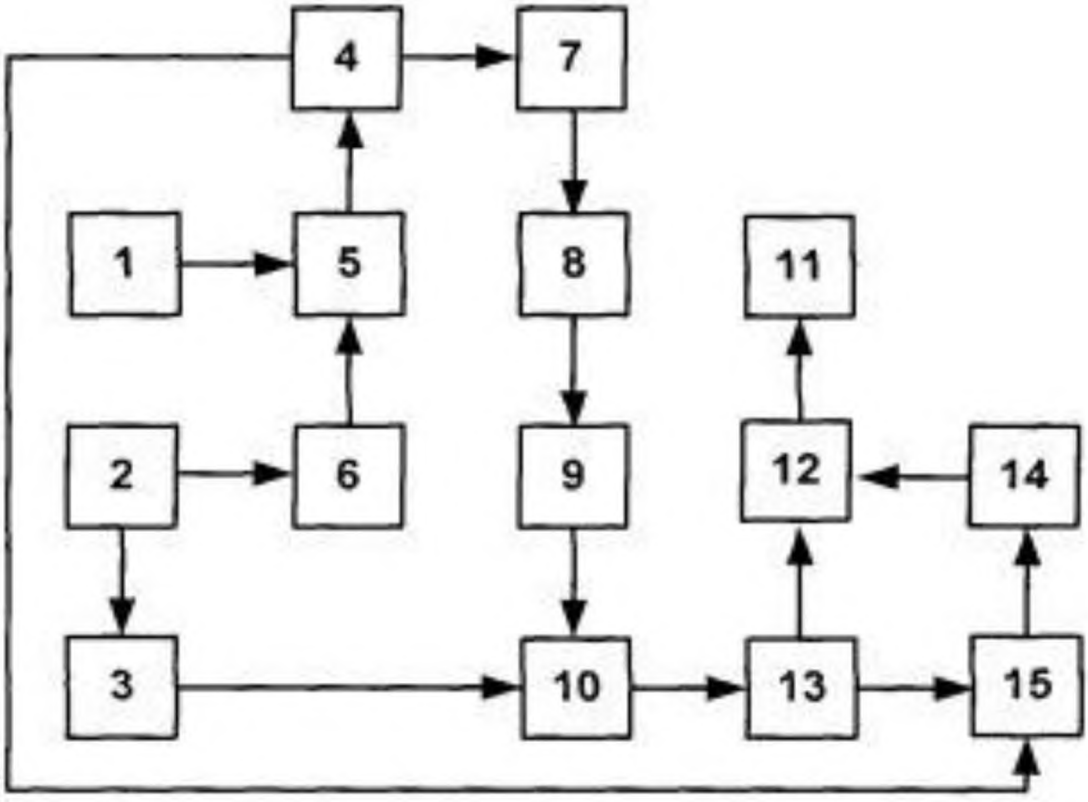

Рисунок 2.1 – Загальна схема пристрою, що реалізує підхід до вбудовування повідомлення в цифрове зображення формату JPEG 2000

Пристрій, що реалізовує запропонований підхід до вбудовування повідомлення в цифрове зображення формату JPEG 2000 (рис. 2.1), працює наступним чином.

Над сигналом цифрового зображення (блок 1) виробляють дискретне вейвлет-перетворення із використанням вейвлет-фільтрів Добеші 9/7 для режиму стиснення із втратами згідно обов'язкової частини стандарту JPEG 2000 (ISO/IEC FCD 15444-1: 2000 (V1.0, 16 March 2000)) (блок 5). Тактові імпульси з блоку 2 – генератора тактових імпульсів подають на вхід блоку 3 (біти вбудованого повідомлення) і на вхід блоку 6 – генератор ПВП (стеганоключ), що визначає номери блоків вейвлет-коефіцієнтів розміром NxN, в які здійснюють вбудовування повідомлення. Сигнал повідомлення подають послідовно побітно на вхід блоку 10 (пристрій порівняння).

Слід підкреслити, що наразі вейвлетне перетворення Добеші 9/7 [11, 13-31, 36-38] є, мабуть, найвідомішим з існуючих на сьогоднішній день вейвлетних перетворень. Більш того, воно вважається одним з найбільш ефективних. Зайвим доказом цього може бути те, що перетворення Добеші 9/7 було вибрано за основу в стандарті для стиснення зображень JPEG2000.

З приходом тактового імпульсу в блоці 6 формують сигнал ПСП (стеганоключ), а на виході блоку генератора ПВП (стеганоключа) формують сигнал, який здійснює вибір сигналу контейнера в блоці 5 і робить передачу сигналу контейнера на вхід блоку 4 (квантувач), де здійснюють процедуру квантування вейвлет-коефіцієнтів. Далі сигнал з першого виходу блоку 4 подають на перший вхід блоку 15 (блок вибору вейвлет-коефіцієнтів з найбільшою дробовою частиною), а з другого виходу блоку 4 подають сигнал на вхід блоку 7 (пристрій нормування), де значення квантування вейвлет-коефіцієнтів округлюють до найменшого цілого згідно з правилом (2.1).

Після вищезазначеного з виходу блоку 7 сигнал подають на вхід блоку 8 (суматор), де визначають значення суми вейвлет-коефіцієнтів в блоці розміром NxN. Далі з виходу блоку 8 сигнал подають на вхід блоку 9 (пристрій для

визначення парності), де визначають парність суми значень вейвлет-коефіцієнтів в блоці розміром NxN.

З виходу блоку 3 на перший вхід блоку 10 (пристрій порівняння) подають один біт вбудованого повідомлення, який порівнюють із сигналом парності суми значень вейвлет-коефіцієнтів з виходу блоку 9, який подають на другий вхід блоку 10. Далі на виході блоку 10 формують сигнал модифікованого контейнера і подають на вхід блоку 13 (комутатор).

При збізі парності суми значень вейвлет-коефіцієнтів сигналу контейнера і біта сигналу вбудованого повідомлення з першого виходу блоку 13 сигнал подають на перший вхід блоку 12 (пристрій для реалізації арифметичного кодування).

При розбіжності парності суми значень вейвлет-коефіцієнтів сигналу контейнера і біта вбудованого повідомлення сигнал з другого виходу блоку 13 подають на вхід блоку 15 (блок вибору вейвлет-коефіцієнта з найбільшою дробовою частиною).

Далі з виходу блоку 15 сигнал подають на вхід блоку 14 (реверсивний лічильник), де значення одного з вейвлет-коефіцієнтів блоку розміром NxN збільшують на одиницю, і на виході блоку 14 формують сигнал модифікованого контейнера, який подають на другий вхід блоку 12. З виходу блоку 12 сигнал подають на вхід блоку 11 (стеганоконтейнер).

Загальна схема пристрою, який реалізує процедуру вилучення повідомлення з цифрового зображення формату JPEG 2000 згідно запропонованого підходу показана на рис. 2.2.

На рис. 2.2 введено такі позначення:

11 – стисле цифрове зображення із вбудованим повідомленням (стеганоконтейнер);

16 – пристрій для реалізації арифметичного декодування;

17 – генератор тактових імпульсів

18 – блок зберігання модифікованих вейвлет-коефіцієнтів;

19 – генератор ПВП (стеганоключ)

20 – вирішальний пристрій;

21 – блок зберігання вилученого повідомлення.

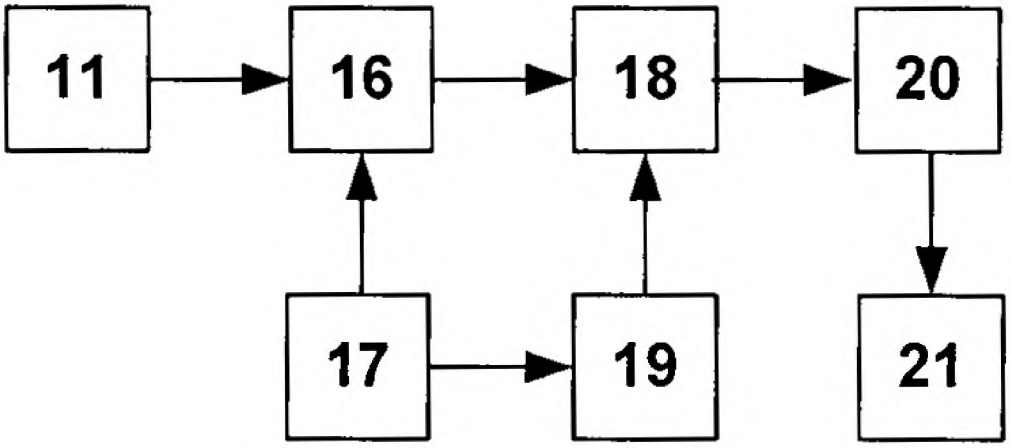

Рисунок 2.2 – Загальна схема пристрою, що реалізує процедуру вилучення повідомлення з цифрового зображення формату JPEG 2000 згідно запропонованого підходу

Вилучення повідомлення, вбудованого в цифрове зображення за запропонованим підходом, загальна схема якого представлена на рис. 2.1, здійснюють відповідно до схеми, представленої на рис. 2.2, в наступному порядку.

Сигнал стисненого цифрового зображення із вбудованим повідомленням (стеганоконтейнер), блок 11, послідовно подають на вхід блоку 16, де над ним здійснюють арифметичне декодування. Тактові імпульси з блоку 17 – генератори тактових імпульсів подають на вхід блоку 16 і на вхід блоку 19 – генератор ПВП (стеганоключ).

З виходу блоку 16 на перший вхід блоку 18 подають сигнал, що формує середньочастотні і високочастотні піддіапазони вейвлет-коефіцієнтів. З виходу блоку 19 формують сигнал, що надходить на другий вхід блоку 18 і здійснює вибір блоків вейвлет-коефіцієнтів розміром NxN у порядку, визначеному ПВП (стеганоключем).

Сигнал із виходу блоку 18 надходить на вхід блоку 20, де здійснюють зчитування вбудованого повідомлення. Після цього з виходу блоку 20 сигнал надходить на вхід блоку 21 – блок зберігання вилученого повідомлення.

2.1 Оцінка ефективності підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації перевірялася за допомогою імітаційних моделей системи-прототипу і системи, що реалізує запропонований підхід.

Моделювання проводилось в програмному середовищі MatLab / Simulink за допомогою стандартного і розробленого програмного забезпечення. Моделювання проводилось за наступних умов:

1) початкове цифрове зображення у форматі BMP;

2) до початкового цифрового зображення застосовують процедуру стиснення за стандартом JPEG 2000 із різними коефіцієнтами стиснення ($К_{ст}$) до процедури арифметичного кодування, а потім застосовують процедуру стиснення за стандартом JPEG 2000 у зворотному порядку до отримання початкового цифрового зображення у форматі BMP;

3) до початкового цифрового зображення застосовують процедуру стиснення за стандартом JPEG 2000 із різними коефіцієнтами стиснення ($К_{ст}$) до процедури арифметичного кодування, потім вбудовують стеганоповідомлення відповідно до запропонованого підходу і застосовують процедуру стиснення за стандартом JPEG 2000 у зворотному порядку до отримання початкового цифрового зображення у форматі BMP;

4) до початкового цифрового зображення застосовують процедуру стиснення за стандартом JPEG 2000 із різними коефіцієнтами стиснення ($К_{ст}$) до процедури арифметичного кодування, застосовують підхід-прототип для вбудовування повідомлення, потім застосовують процедуру стиснення за стандартом JPEG 2000 у зворотному порядку до отримання початкового цифрового зображення у форматі BMP.

В якості оцінки рівня спотворень вибирають пікове співвідношення сигнал / шум (PSNR – Peak Signal-to-Noise Ratio):

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right), \quad (2.2)$$

де MAXI – максимальне значення, яке приймається пікселем цифрового зображення;

MSE – середньоквадратичне відхилення, яке обчислюють за формулою:

$$MSE = \frac{1}{m \times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left|I(i, j) - K(i, j)\right|^2 \quad (2.3)$$

де I(i, j) і K(i, j) – поточне й оцінюване цифрове зображення, відповідно;

m×n – розмір цифрового зображення.

Далі за формулою (2.2) обчислюють PSNR:

1) для чистого цифрового зображення по відношенню до початкового цифрового зображення;

2) для цифрового зображення з повідомленням, вбудованим згідно запропонованого підходу стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації;

3) для цифрового зображення з повідомленням, вбудованим згідно підходу-прототипу.

Дана оцінка буде об'єктивною у разі рівних умов для стеганоалгоритмів. Під рівними умовами розуміється однаковий ступінь стиснення цифрових зображень і рівний обсяг вбудованої інформації.

Результати оцінки ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації представлено графічно на рис. 2.3.

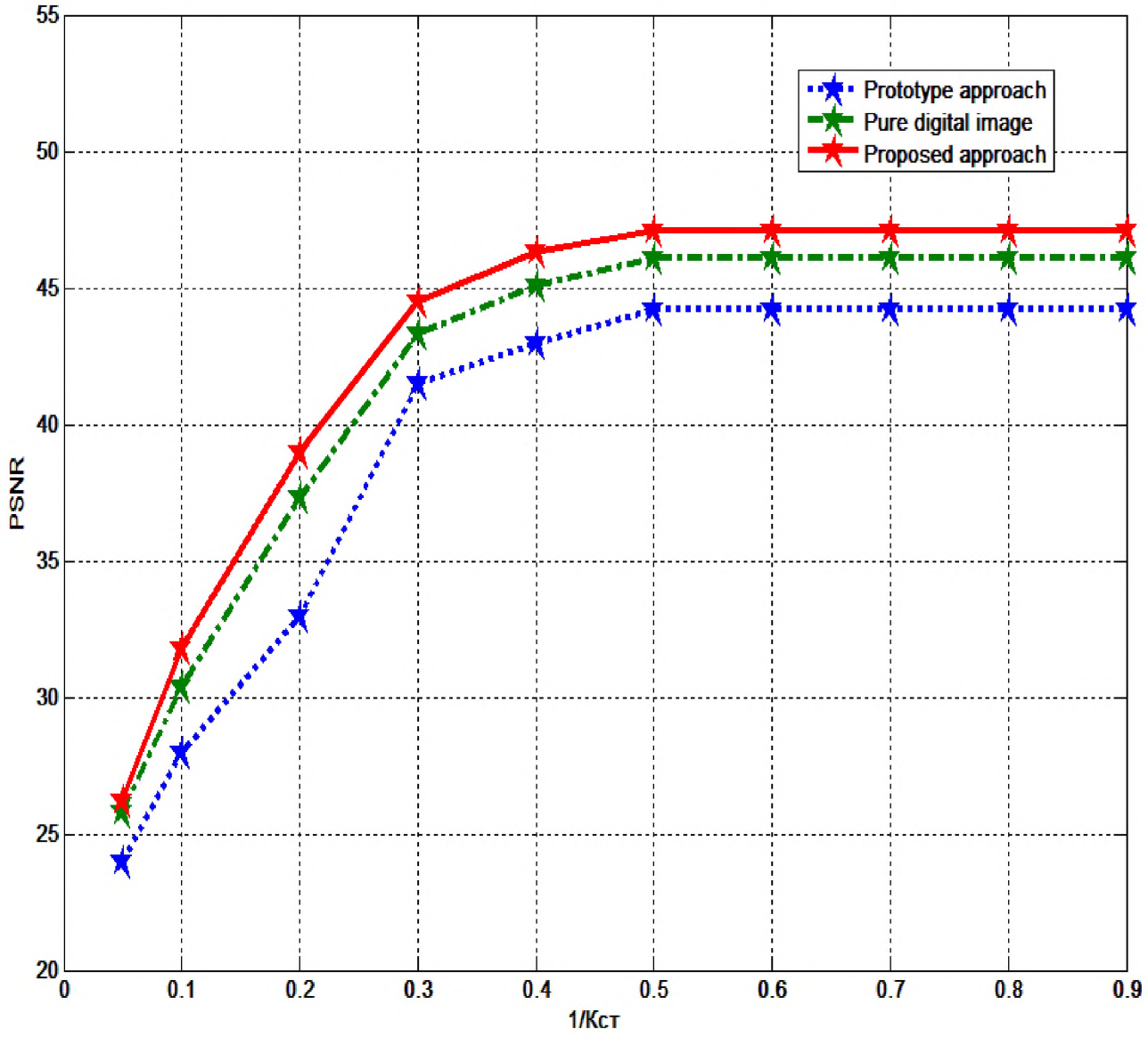

Рисунок 2.3 – Результати оцінки ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації

В результаті моделювання (рис. 2.3) встановлено, що застосування запропонованого підходу дає виграш по PSNR при рівних умовах на 3-4 дБ (в

залежності від коефіцієнта стиснення ($К_{ст}$) у цифровому форматі) у порівнянні із підходом-прототипом.

Проведене моделювання показало високу стійкість запропонованого підходу до вбудовування повідомлення в цифрове зображення формату JPEG 2000 проти візуального аналізу і статистичних методів аналізу розподілів найменш значущих бітів зображення. В ході моделювання відносний обсяг впроваджених даних в ряді випадків становив 30% від обсягу початкового цифрового зображення, при повному збереженні візуальної якості останнього. Для забезпечення найбільшої ефективності вбудовування в цифрове зображення повідомлення останньому надається характер псевдовипадкової послідовності. Найбільш ефективним є використання запропонованого підходу до вбудовування інформації спільно із алгоритмами скремблювання і ефективного кодування.

Практична придатність запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації обумовлена тим, що пристрій, який реалізує запропонований підхід, може бути реалізований за допомогою сучасної елементної бази, із досягненням зазначеного у запропонованому підході призначення.

2.3 Висновки

Запропонований підхід відноситься до області стеганографії, а саме до способів вбудовування повідомлення в цифрові зображення. Технічний результат полягає в забезпеченні можливості збереження цілісності впровадженої інформації. Метою розробки підходу є зменшення оцінки рівня спотворень цифрового зображення формату JPEG 2000.

Завданням запропонованого підходу є таке вбудовування повідомлення в цифрове зображення формату JPEG 2000, яке забезпечує можливість збереження цілісності впровадженої інформації при передачі останньої по

відкритих каналах зв'язку. Запропонований підхід заснований на кодуванні бітів вбудованого повідомлення сумою значень вейвлет-коефіцієнтів в блоці розміром N×N з області средньочастотних і високочастотних піддіапазонів вейвлет-перетворення. При цьому вибір розміру блоку залежить від вимог, що пред'являються до стеганосистеми: а саме, чим більше розмір блоку, тим вище стійкість стеганосистеми.

Дане завдання вирішується тим, що спосіб вбудовування повідомлення в цифрове зображення формату JPEG 2000 здійснюють після процедури квантування в блоки вейвлет-коефіцієнтів розміром NxN, причому значення бітів вбудованого повідомлення кодують парністю суми значень вейвлет-коефіцієнтів в блоці. При цьому, якщо значення вбудованого біта не збігається з парністю суми значень вейвлет-коефіцієнтів в блоці, значення одного з них збільшують на одиницю, причому для модифікації вибирають вейвлет-коефіцієнт, значення якого має найбільшу дробову частину.

Запропонований підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації була проведена шляхом моделювання в середовищі Matlab / Simulink.

Встановлено, що застосування запропонованого підходу дає виграш по PSNR при рівних умовах на 3-4 дБ (в залежності від коефіцієнта стиснення ($К_{ст}$) у цифровому форматі) у порівнянні із підходом-прототипом.

Проведене моделювання показало високу стійкість запропонованого підходу до вбудовування повідомлення в цифрове зображення формату JPEG 2000 проти візуального аналізу і статистичних методів аналізу розподілів найменш значущих бітів зображення. В ході моделювання відносний обсяг впроваджених даних в ряді випадків становив 30% від обсягу початкового

цифрового зображення, при повному збереженні візуальної якості останнього. Для забезпечення найбільшої ефективності вбудовування в цифрове зображення повідомлення останньому надається характер псевдовипадкової послідовності.

Найбільш ефективним є використання запропонованого підходу до вбудовування інформації спільно із алгоритмами скремблювання і ефективного кодування.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є обґрунтування економічної доцільності стеганографічного вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів. Досягнення цієї мети потребує здійснення визначення величини капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту від впровадження запропонованих заходів; показників економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальними витрати називаються тому, що робляться, як правило, один раз, на початкових етапах створення ІС. До капітальних слід відносити наступні витрати: вартість розробки і впровадження проекту; залучення зовнішніх консультантів; первинні закупівлі основного ПЗ; первинні закупівлі додаткового ПЗ; первинні закупівлі апаратного забезпечення тощо.

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 вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів

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 вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів, $t_{тз}$=23;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=40;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=30;

$t_р$ – тривалість розробки підходу щодо стеганографічного вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів, $t_м$=50;

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

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 23+40+30+50+10 = 153 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо стеганографічного вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів

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 $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 22338+650,25 = 22998,25 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 153*146 = 22338 \text{ грн.}$$

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:

$$З_{мч} = t*С_{мч}=153*4,25=650,25 \text{ грн.}$$

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:

$$C_{мч} = 0{,}8 \cdot 2 \cdot 1{,}55 + \frac{5120 \cdot 0{,}4}{1920} + \frac{4187 \cdot 0{,}2}{1920} = 4{,}25 \text{ грн.}$$

Оцінка ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації була 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 3000 грн.

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

$$К=К_{рп}+К_{зпз}+К_{пз}+К_{аз}+К_{навч}+К_{н}=22998{,}25+3000=225998{,}25 \text{ грн.}$$

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:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.}$$

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.).

Оскільки середовищі Matlab/Simulink, яке використовується для оцінки ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації вже використовується, 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 8000 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 16000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки. Отже,

$$С_з = (16000*12 + 16000*12*0,08)*0,2 = 41472 \text{ грн.}$$

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

$$С_{єв} = 41472*0,22 = 9123,84 \text{ грн.}$$

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=0,8 кВт);

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

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

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

$$С_{ел} = 0,8*2*1920*1,55 = 4761,6 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 225998,25*0,01=2259,98 грн).

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

$$С_к = 8000+41472+9123,84+4761,6+2259,98 = 65617,42 \text{ грн.}$$

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

$$С = 65617,42 \text{ грн.}$$

3.2 Оцінка можливого збитку

Запропонований підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

Оцінка величини можливого збитку визначатиметься для умовного підприємства, яке може передавати інформацію по відкритих каналах зв'язку, вартість якої потенційно складає 500000 грн. Вірогідність реалізації загроз (R) щодо цифрових зображень формату JPEG 2000, які можуть порушити цілісності інформації, складає 70%.

Отже, можлива величина збитку (В) на рік від загроз щодо цифрових зображень формату JPEG 2000, які можуть порушити цілісність інформації, становитиме:

$$B = 500000*0,7 = 350000 \text{ грн.}$$

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

R – вірогідність успішної реалізації загрози (70%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 350000 - 65617,42 = 284382,6 \text{ грн.}$$

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 (То).

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:

$$ROSI = \frac{284382,6}{225998,25} = 1,26, \quad \text{частки одиниці,}$$

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:

$$1,26 > (6 - 5)/100 = 1,26 > 0,01.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,26} = 0,79 \text{ років (біля 9,5 місяців).}$$

3.4 Висновок

Таким чином, обґрунтування економічної доцільності стеганографічного вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів можна вважати економічно доцільним. У разі використання запропонованого підходу стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації може дозволити отримати економічний ефект у розмірі 284382,6. Капітальні витрати складають 225998,25 грн., експлуатаційні – 284382,6 грн. Коефіцієнт повернення інвестицій складає 1,26 грн./грн., тобто 1,26 грн. економічного ефекту на 1 грн. капітальних витрат. Термін окупності – менше року (0,79 років).

ВИСНОВКИ

1. В результаті аналізу принципи впровадження інформації у нерухомі зображеннях, а також вейвлет-перетворень встановлено, що серед методів приховування найпоширенішими наразі є методи на основі вейвлет-перетворення. Ці методи є популярними, оскільки не вносять значних спотворень у зображення, мають достатню пропускну здатність та є стійкими до навмисних атак та викривлень у каналах зв'язку.

2. В результаті аналізу існуючих підходів до вбудовування додаткової інформації у цифрові зображення встановлено їх недоліки. Недоліком відомих підходів до впровадження інформації в цифрові зображення [32-34] є неможливість їх застосування для графічних зображень стислих форматів, зокрема JPEG і JPEG 2000. В основі даних форматів лежать алгоритми стиснення зі втратами, які у свою чергу мають деградуючий вплив на впроваджувану інформацію. Недоліком відомого підходу до створення водяних знаків для цифрових зображень і відео (прототипу) [35] є часткова втрата інформації, що вбудовується, при стисненні за стандартом JPEG 2000 під час процедури квантування, а також обмежений обсяг вбудованого повідомлення внаслідок обмеженої кількості вейвлет-коефіцієнтів з великими значеннями в середньочастотних і в високочастотних піддіапазонах області вейвлет-перетворення.

3. Запропоновано підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації, який заснований на кодуванні бітів вбудованого повідомлення сумою значень вейвлет-коефіцієнтів в блоці розміром $N \times N$ з області средньочастотних і високочастотних піддіапазонів вейвлет-перетворення. При цьому вибір розміру блоку залежить від вимог, що пред'являються до стеганосистеми: а саме, чим більше розмір блоку, тим вище стійкість стеганосистеми. Метою розробки підходу є зменшення оцінки рівня спотворень цифрового зображення формату JPEG 2000. Це досягається тим, що

вбудовування повідомлення в цифрове зображення формату JPEG 2000 здійснюють після процедури квантування в блоки вейвлет-коефіцієнтів розміром $N \times N$, причому значення бітів вбудованого повідомлення кодують парністю суми значень вейвлет-коефіцієнтів в блоці. При цьому, якщо значення вбудованого біта не збігається з парністю суми значень вейвлет-коефіцієнтів в блоці, значення одного з них збільшують на одиницю, причому для модифікації вибирають вейвлет-коефіцієнт, значення якого має найбільшу дробову частину.

4. Результат оцінки ефективності запропонованого підходу до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації у порівнянні із підходом-прототипом доводить ефективність запропонованого підходу, а саме – зменшення оцінки рівня спотворень цифрового зображення формату JPEG 2000. Встановлено, що застосування запропонованого підходу дає виграш по PSNR при рівних умовах на 3-4 дБ (в залежності від коефіцієнта стиснення ($К_{ст}$) у цифровому форматі) у порівнянні із підходом-прототипом. В ході моделювання відносний обсяг впроваджених даних в ряді випадків становив 30% від обсягу початкового цифрового зображення, при повному збереженні візуальної якості останнього. Для забезпечення найбільшої ефективності вбудовування в цифрове зображення повідомлення останньому надається характер псевдовипадкової послідовності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кузнецов О.О. Стеганографія : навчальний посібник / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

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

3. Хорошко, В.А. Методы и средства защиты информации: научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. – К. : ЮНИОР, 2003. – 505 с.

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

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

6. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. Учебное пособие. / С. Уэлстид. – М.: Издательство Триумф, 2003. – 320 с.

7. Миано Дж. Форматы и алгоритмы сжатия изображений в действии. – М.: Изд-во «Триумф», 2003. – 320 с.

8. Гонсалес Р. Цифровая обработка изображений (перевод с английского) / Р. Гонсалес, Р. Вудс, под ред. П.А. Чочиа – М.: Техносфера, 2005. – 1072 с.

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

10. Shapiro J. Embedded image coding using zerotrees of wavelet coefficients / J. Shapiro // IEEE Trans. on Signal Processing. 1993. – № 12. – P. 3445-3462.

11. Taubman D. Embedded block coding in JPEG 2000 / D. Taubman, E. Ordentlich, M. Weinberger, G. Seroussi // Signal Processing: Image Communication. 2002. – №17. – P. 49-72.

12. Shoham Y. Efficient bit allocation for an arbitrary set of quantizers / Y. Shoham, A. Gersho // IEEE Trans. Acoustics, Speech, and Signal Processing. 1988. – № 9. – P. 1445-1453.

13. Добеши И. Десять лекций по вейвлетам. / И. Добеши. И: НИЦ «Регулярная и хаотическая динамика», 2001. – 464 с.

14. Юдин М.Н. Введение в вейвлет-анализ: Учеб.-практическое пособие. / М.Н. Юдин, Ю.А. Фарков, Д.М. Филатов. – М.: Моск. геологоразв. акад. – 2001. – 72 с.

15. Новиков Л.В. Основы вейвлет-анализа сигналов. Учебное пособие. / Л.В. Новиков. – СПб.: Изд. ООО “МОДУС+”. – 1999. – 152 с.

16. Фарков Ю.А. Ортогональные всплески на локально компактных абелевых группах. / Ю.А. Фарков. // Функциональный анализ и его приложения, №4. – 31 (1997).

17. Cohen A. Non-separable bidimensional wavelet bases. / A. Cohen, I. Daubechies. // Revista Matematica Iberoamericana. – №1, 9 (1993).

18. Daubechies I. Orthonormal Bases of compactly supported wavelets. / I. Daubechies // Comm. PureAppl. Math. – 1988. – № 41. – 909-996 pp.

19. Daubechies Ed. I. Different pespectives on Wavelets. / Ed. I. Daubechies. – American Mathematical Society. Short Course. – San Antonio, Texas. – 1993.

20. Gagnon L. Symmetric Daubechies' wavelets and numerical solutions of NLS2 equations. / L. Gagnon, J.M. Lina. // J. Phys. A: Math. – Gen. 27, 1994, –8207-8230 pp.

21. Hoekstra E.V. Multiscale Analisys of seismic data by the wavelet transform. M. Sc. Thesis. Delft, 1996.

22. Jaerth B. An Owerview of Wavelet Based Multiresolution Analyses. / B. Jaerth, W. Swedlens. // SIAM Review. – 1994. – Vol.36. –377-412 pp.

23. Kaiser J. A Friendly Guide to Wavelets. Birkhauser. ISBN G-8176-3711-7, Boston, 1994.

24. Mallat S. Multiresolution approximation and wavelets. Trans.Amer. Mayh. Soc. 315, 1989, pp.69-88.

25. Meyer Y. Wavelets: Algorithms and Applications. / Y. Meyer. – SIAM, Philadelphia, 1993. – 133 p.

26. Numerical Recipes. // Cambrige University Press, 1992-1998. – ISBN 0-521-43108-5.

27. Priezzhev V.B. Self-Similar Systems. / V.B. Priezzhev, V.P. Spiridonov. – Dubna, 1999.

28. Resnikoff H.L. Wavelet Analysis. / H.L. Resnikoff, R.O. Wells. – Springer, 1991.

29. Ruskai M.B. Wavelets and their Applications. / M.B. Ruskai. – Boston: Ed. Jones and Barlett. – 1992. – 474 p.

30. Buckheit J. WaveLab and Reproducible Research. / J. Buckheit, D. Donho. // Wavelets in Statistics. – New York : Springer Verlag. – 55-82 pp.

31. Chui C. An Introduction to Wavelets. / Charles K. Chui, Jeffrey M. Lemm, Sahra Sedigh. – San Diego, CA : Academic Press, 1992. – 264 p.

32. Provos N. Defending Against Statistical Steganalysis / N. Provos // Proceeding of the 10 USENIX Security Symposium, 2001. – P.323-335.

33. Патент РФ 2288544. Способ внедрения дополнительной информации в цифровые изображения / А.Т. Алиев – заявл. 25.04.2004, опубл. 27.11.2006.

34. Патент РФ 2407216. Способ встраивания сообщения в цифровое изображение / С.В. Захаркин, И.В. Иванов, Д.А. Кирюхин, М.В. Воропаев, А.В. Болбенков – заявл. 29.06.2009, опубл. 20.12.2010.

35. Patent US 6556689. Watermarking methods for digital images and videos / Xiang-Gen Xia, Charles Boncelet, Jr., Gonzalo R. Arce – application 20.04.1999, publication 29.03.2003.

36. Хорошко В.О. Основи комп'ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця: ВДТУ, 2003. – 143 с.

37. Ouled-Zaid A., Makhlou A., Olivier C. Improved QIM-Based Watermarking Integrated to JPEG2000 Coding Scheme // Springer journal of Signal, Image and Video Processing – 2009. – Vol. 3, P. 197-207.

38. Fan Y., Chiang A., Shen J. ROI-based watermarking scheme for JPEG 2000 // Springer journal of Circuits, Systems, and Signal Processing 27(5). – 2008. – P. 763-774.

39. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

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	34	
6	А4	Спеціальна частина	12	
7	А4	Економічний розділ	7	
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 Астахов.ppt

2 Диплом Астахов.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 125-18зск-1 Астахова О.О. на тему: «Стеганографічне вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 73 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на зменшення оцінки рівня спотворень цифрового зображення формату JPEG 2000.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів впровадження інформації у нерухомі зображення та вейвлет-перетворень, а також існуючих підходів до вбудовування додаткової інформації у цифрові зображення в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до стеганографічного вбудовування повідомлення в цифрове зображення формату JPEG 2000 із збереженням цілісності впровадженої інформації та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

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

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