Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)
(рівень вищої освіти)

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СТРУКТУРНОГО СТЕГАНОГРАФІЧНОГО КОДУВАННЯ З ВИЯВЛЕННЯМ КОНТУРНОЇ ІНФОРМАЦІЇ
(тема)

Виконав: студент 2 курсу, групи СКСм-18-2
Бараннік Д.В.
(прізвище, ініціали)
Спеціальність 123_ Комп'ютерна інженерія
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Спеціалізовані комп'ютерні системи
(повна назва освітньої програми)
Керівник
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри АПОТ _____ Чумаченко С.В.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління

Кафедра Автоматизації проектування обчислювальної техніки

Рівень вищої освіти другий (магістерський)

Спеціальність 123 – Комп'ютерна інженерія

Тип програми Освітньо-професійна

Освітня програма Спеціалізовані комп'ютерні системи

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2019 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Баранніку Дмитру Володимировичу

(прізвище, ім'я, по батькові)

1. Тема роботи Метод захисту інформації на основі структурного стеганографічного кодування з виявленням контурної інформації

затверджена наказом по університету від ____ _____20__ р. № _____

2. Термін подання студентом роботи до екзаменаційної комісії 01 грудня 2019 р.

3. Вихідні дані до роботи Необхідно вирішити такі задачі: 1) вибір методу стеганографічних перетворень; 2) розробка технології функціонального перетворення чисел з імплантованими даними на основі нерівновагового позиційного кодування; 3) розробка моделі структурного стеганографічного кодування; 4) розробка програмного забезпечення для реалізації запропонованої технології.

4. Перелік питань, що потрібно опрацювати в роботі 1) Огляд літератури за темою дослідження; 2) Розгляд методів безпосереднього стеганографічного вбудовування для відеоконтейнера; 3) Аспекти вдосконалення технологій безпосереднього стеганографічного вбудовування; 4) Розробка методу структурного стеганографічного кодування; 4) Оцінка характеристик ефективності функціонування розробленого методу стеганографічного кодування; 5) Розробка програмного забезпечення для реалізації запропонованої технології.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

Презентація _____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Змістовна частина	Проф. каф. АПОТ Литвинова Є.І.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	10.09.2019	
2	Аналіз предметної області	20.09.2019	
3	Аналіз джерел з проблемної галузі	15.10.2019	
4	Опис методу безпосереднього стеганографічного вбудовування для	20.10.2019	
5	Опис методологічних аспектів вдосконалення технологій безпосереднього стеганографічного вбудовування	20.10.2019	
6	Розробка методу структурного стеганографічного кодування	30.10.2019	
7	Оцінка характеристик ефективності функціонування розробленого методу стеганографічного кодування	20.11.2019	
8	Розробка програмного забезпечення	28.11.2019	
9	Оформлення пояснювальної записки та графічного матеріалу	01.12.2019	
10	Представлення роботи до перевірки в системі	01.12.2019	
11	Представлення роботи до захисту	09.12.2019	

Дата видачі завдання _____

Студент _____
(підпис)

Керівник роботи _____ _____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи бакалавра: містить 130 с. основного тексту, 40 рис., 7 табл., 3 дод., 9 джерел.

КОДУВАННЯ, СТЕГАНОГРАФІЯ, ЗОБРАЖЕННЯ, БЕЗПЕКА, ОБРОБКА, СТІЙКІСТЬ.

Метою атестаційної роботи є розробка теоретичних основ і методів підвищення безпеки спеціальної інформації на основі стеганографічного перетворення.

У ході виконання атестаційної роботи було розглянуто існуючі методи стеганографічних перетворень та проведено аналіз їх недоліків. Розроблено технологію функціонального перетворення чисел з імплантованими даними на основі нерівновагового позиційного кодування та модель структурно-комбінаторного стеганографічного кодування з маскуванням. Розроблене програмне забезпечення для реалізації запропонованої технології.

ABSTRACT

Bachelor Diploma Thesis contains: 130 pages of the main text, 40 figures, 7 tables, 3 annexes, 9 references.

CODING, STEGANOGRAPHY, PICTURE, SECURITY, TREATMENT, DURABILITY.

The purpose of the Bachelor Diploma is the development of theoretical background and methods for improving the safety of special information based on steganographic transformation.

Existing methods of steganographic transformation were considered in the work; analysis of their diadvantages is carried out. A technology for the functional transformation of numbers with implanted data based on non-equilibrium positional coding and the model of structurally-combinatorial steganographic coding with masking are proposed. Software for the implementation of the proposed technology is developed.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДКП – дискретне косинусне перетворення

ЗК – зображення-контейнер

НЗБ – найменш значимий біт

НПЧ – нерівновагове позиційне число

РС – розширення спектру

СКП – системи критичного призначення

ЗМІ – засоби масової інформації

СКІ – системи критичної інфраструктури

СІР – спеціальні інформаційні ресурси

ПВСШ – пікове відношення сигнал\шум

ВСТУП

Досвід функціонування систем критичної інфраструктури в умовах активної протидії противника виявив гостру потребу забезпечення необхідного рівня безпеки спеціальних інформаційних ресурсів (СІР). З одного боку це диктується підвищеною значущістю СІР для інформаційної підтримки процесів ухвалення рішень, у тому числі в кризових ситуаціях. З іншого боку підвищуються загрози порушення конфіденційності та цілісності СІР. У значній мірі це обумовлено зростанням оперативно-програмних і інформаційно-технологічних можливостей протиборчої сторони. Тому підвищення безпеки спеціальних інформаційних ресурсів в інфокомунікаційних системах є актуальним напрямом науково-прикладних досліджень.

Звідси виникає інтерес розробки нових шляхів забезпечення безпеки СІР. Одним з напрямів є використання стеганографічних методів вбудовування інформації в зображення-контейнер. Базою для реалізації такого підходу є системи відеоконференцзв'язку, широке використання мультимедійних засобів, розвиток поля відеоінформації, наявність прив'язки службової інформації до конкретного відеоматеріалу.

Серед методів стеганографічних перетворень окремий інтерес представляють методи безпосереднього вбудовування інформації в зображення-контейнер.

Проведений аналіз існуючих методів виявив такі проблемні недоліки:

- недостатнє значення відносної стеганографічної ємності;

- недостатнє значення стійкості вбудовуваних даних до атак противника;

- значні візуальні спотворення стеганограми.

Такі недоліки обумовлені тим, що в процесі стеганографічних перетворень в основному враховуються психовізуальні закономірності. При

цьому вилучення вбудовуваної інформації здійснюється з використанням кореляційних залежностей, які порушуються в результаті нелінійної обробки стеганограми.

У цей же час підвищуються вимоги до інформаційного забезпечення систем критичної інфраструктури (СКІ). Такі вимоги обумовлені наступними чинниками:

- підвищення інформаційної інтенсивності донесень в умовах кризових ситуацій;

- використання в якості спеціальних донесень відеоматеріалів;

- підвищення значимості впливу спеціальних донесень на результативність функціонування СКІ;

- підвищення вимог відносно достовірності і наочності донесень;

- необхідність оперативної доставки прихованих повідомлень в обмежені тимчасові проміжки сеансу зв'язку;

- необхідність забезпечення і контролю використання пропагандистського поля протистояння.

В процесі використання існуючих стеганографічних систем для прихованої передачі спеціальної інформації виникає протиріччя, яке полягає в тому, що існуючі стеганографічні технології не забезпечують повною мірою системних вимог в кризових ситуаціях в умовах наявності активних протиборчих сторін.

Для вирішення протиріччя в процесі побудови стеганографічних систем пропонується додатково враховувати наявність структурних закономірностей відеоконтейнерів.

Таким чином метою досліджень є розробка методу підвищення безпеки спеціальної інформації для інформаційно-комунікаційних систем критичного призначення на основі стеганографічних перетворень.

1 АСПЕКТИ АКТУАЛЬНОСТІ І ЗНАЧУЩОСТІ СТЕГАНОГРАФІЧНИХ ПІДХОДІВ

Для обґрунтування підходу відносно підвищення безпеки спеціальних інформаційних ресурсів на основі стеганографічних методів необхідно розглянути аспекти, які визначають їх актуальність і значущість в кризових умовах [1]. Тут слід виділити такі аспекти актуальності і значущості стеганографічних методів:

а) необхідність підвищення рівня конфіденційності, цілісності і доступності спеціального інформаційного ресурсу. У сучасних умовах функціонування систем кризового призначення необхідною умовою є забезпечення заданого рівня складових інформаційної безпеки: конфіденційності, цілісності і доступності;

б) обмеження при використанні криптографічних алгоритмів захисту спеціальних інформаційних ресурсів. Вони мають негативні наслідки і можуть завдати збитки політичному і економічному іміджу держави;

в) формування умов для розвитку стеганографічних підходів забезпечення безпеки спеціальних інформаційних ресурсів обумовлюються наступними позиціями:

– наявністю великої кількості різних стеганографічних методів прихованого вбудовування і передачі інформації;

– розвитком телекомунікаційних технологій, що використовують відкриті канали передачі даних широкого доступу;

– відсутністю достатньої кількості методів стеганографічного аналізу для виявлення фактів наявності прихованого вбудовування спеціальної інформації;

– широким поширенням мультимедійних файлів в інфокомунікаційному просторі. Це створює базу для формування контейнерів, які використовуються при вбудовуванні інформації;

– д) відсутністю обмежень в нормативно-правовій базі на використання стеганографічних методів захисту інформації.

Тому в системах комплексного захисту спеціальних інформаційних ресурсів потрібно також використовувати методи стеганографічних перетворень. Стеганографічні перетворення на відміну від криптографічної обробки дозволяють приховати сам факт наявності секретного повідомлення. Тут інформація у вигляді повідомлення перетворюється певним чином і вбудовується в деякий цифровий контейнер, який не привертає уваги. Функціональна схема реалізації прихованої передачі даних на основі використання стеганографічних підходів представлена на рис 1.6 і передбачає такі етапи:

1. Стеганографічне вбудовування. На цьому етапі здійснюється стеганографічне вбудовування інформації в цифровий контейнер. Вбудовуване повідомлення може бути заздалегідь перетворене на основі алгоритмів шифрування, компресійного і завадостійкого кодування. У стеганографічному кодері перетворене повідомлення вбудовується в контейнер на основі стеганографічного правила і ключової інформації.

В результаті стеганографічного перетворення формується стеганограма.

2. Передача стеганографічно перетвореного контейнера (стеганограми) отримувачу по каналах передачі даних або розміщення стеганограми в сховищах. В процесі передачі в інфокомунікаціях стеганограма може піддаватися активним пасивним діям.

3. Стеганографічне вилучення. На цьому етапі авторизований користувач проводить стеганографічне декодування. В цьому випадку йому відома наступна інформація:

- факт наявності вбудованої інформації в стеганограмі;
- правило стеганографічного декодування;
- ключова інформація.

В результаті зворотнього стеганографічного перетворення авторизований користувач здійснює вилучення вбудованої інформації.

Процес стеганографічного вилучення здійснюється за наявності на приймальній стороні ключової інформації.

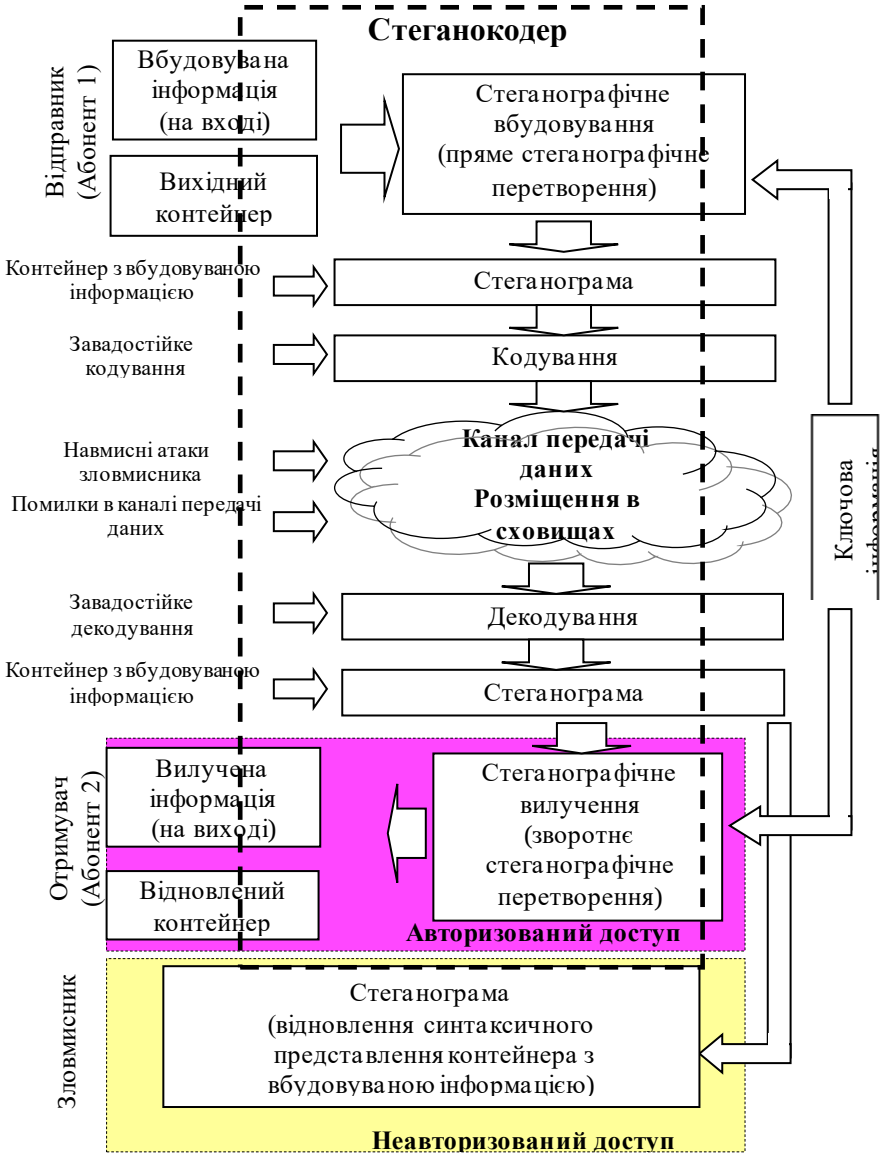

Рисунок. 1.1 – Функціональна схема реалізації прихованої передачі даних на основі стеганографічного підходу

Тепер розглянемо випадок для неавторизованого доступу. Тут у зловмисника відсутня інформація про наявність скритного вбудовування повідомлення в конкретній стеганограмі. Навіть якщо зловмисник обізнаний про те, що в даній стеганограмі присутні вбудовані дані, він не здатний їх вилучити внаслідок відсутності у нього ключової інформації.

2 МЕТОДИ БЕЗПОСЕРЕДНЬОГО СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ ДЛЯ ВІДЕОКОНТЕЙНЕРА

2.1 Формування показників якості функціонування стеганографічних систем

Для порівняння і оцінки існуючих стеганографічних систем розглянемо показники ефективності їх функціонування. Перша група показників характеризує стеганографічний метод з позиції скритності, тобто стійкості стеганографічного перетворення до виявлення факту наявності в зображенні скритного вбудовування. Розгляд скритності можливий по таких складових:

1. Ймовірність $P_{уст}$ встановлення зловмисником факту наявності секретного повідомлення в зображенні. Чим ближче значення величини $P_{уст}$ до нуля тим вища стійкість стеганографічного методу до виявлення факту наявності вбудованих даних [2].

Ці показники базуються на обчисленні метрики $\varepsilon(A;A')$, яка вказує на ступінь відмінності між контейнером-оригіналом і стеганозображенням. До них відносяться:

2. Пікове відношення сигнал-шум h зображення з вбудованими даними при неавторизованому доступі. Дана величина характеризує візуальні спотворення, які вносяться до зображення-контейнера в процесі вбудовування, і визначається на основі наступної формули:

$$h = 20\lg\left(\frac{255}{\sigma}\right) \text{ (дБ)}, \qquad (2.1)$$

де σ – середньоквадратичне відхилення зображення з вбудованими даними відносно зображення-контейнера.

3. Ймовірність $P_{бл}$ правильного визначення блоку зображення з вбудованою інформацією. Противником можуть робитися спроби визначення блоку зображення з вбудованими даними. Чим ближче значення величини до нуля, тим вищою є стійкість стеганографічного методу відносно правильного виявлення зловмисником блоку зображення з вбудованими даними.

4. Ймовірність $P_{стег}$ правильного вилучення вбудованого повідомлення зловмисником із стеганограми. При відомому факті наявності інформації в зображенні, противником може бути зроблена спроба вилучення вбудованих даних. При ймовірності $P_{стег}$, що дорівнює нулю, стеганографічний метод є стійким до правильного вилучення приховуваних даних – це ідеальні умови.

Друга група показників характеризує метод стеганографічного перетворення з позиції об'єму вбудовуваних даних.

Методи стеганографії можуть бути оцінені за об'ємом вбудовуваних даних. Об'єм вбудовуваних даних може бути представлений наступними показниками:

1. Відносна стеганографічна ємність $W_{\text{відн}}$ стеганографічної системи. Величина $W_{\text{відн}}$ відносної стеганографічної ємності системи визначається на основі наступної формули:

$$W_{\text{відн}} = \frac{W_{\text{вбуд}}}{W_{\text{вих}}}. \tag{2.2}$$

У відсотках значення відносної стеганографічної ємності системи оцінюється на основі наступного виразу:

$$W_{\text{відн}} = \frac{W_{\text{вбуд}}}{W_{\text{вих}}} * 100\%. \tag{2.3}$$

2. Стеганографічний бітрейт S_b - величина, що визначає кількість пікселів в середньому необхідних для вбудовування одного біта інформації. Вимірюється в бітах на піксель, біт/піксель. Відповідна оцінка має вигляд:

$$S_b = \frac{w_{встр}}{Z_{\min,стр} Z_{\min,стб}}, \quad (2.4)$$

де S_b - стеганографічний бітрейт, біт/піксель;

$w_{встр}$ - об'єм вбудовуваної інформації, вимірюється в бітах;

$Z_{\min,стр} Z_{\min,стб}$ - мінімально необхідний розмір зображення, достатній для вбудовування інформації об'ємом $w_{встр}$ на основі оцінюваного стеганографічного алгоритму.

3. Ймовірність $P_{\text{вил}}$ безпомилкового вилучення вбудованих даних авторизованим користувачем. Ймовірність $P_{\text{вил}}$ визначається на основі наступного виразу:

$$P_{\text{вил}} = \frac{W_{\text{вил}}}{W_{\text{вбуд}}}, \quad (2.5)$$

де $W_{\text{вбуд}}$ - об'єм вбудовуваної інформації, біт;

$W_{\text{вил}}$ - об'єм безпомилково вилученої інформації, біт.

Третя група показників характеризує стеганографічний метод з позиції часових затрат на реалізацію прямого і зворотнього стеганографічного перетворення.

Четверта група показників характеризує стеганографічний метод з позиції стійкості до атак.

П’ята група показників характеризує стеганографічні методи з позиції зміни значень показників ефективності компресійного представлення зображення-контейнера в умовах наявності вбудованих даних відносно варіанту відсутності вбудованої інформації.

Пропонується ввести наступні показники оцінки впливу стеганографічних перетворень на показники компресійного представлення зображення-контейнера:

1. Ступінь Δh зміни пікового відношення сигнал-шум, як результат модифікації елементів зображення-контейнера:

$$\Delta h = | h_{исх} - h |, \tag{2.6}$$

де $h_{исх}$ - пікове відношення сигнал-шум контейнера-зображення, дБ;

h - пікове відношення сигнал-шум зображення з вбудованою інформацією, дБ.

2. Коефіцієнт Δk зниження ступеня стиснення зображення з вбудованими даними при заданому значенні h пікового відношення сигнал-шум. Це задається формулою:

$$\Delta k = \frac{W_{сж}}{W'_{сж}}, \tag{2.7}$$

де $W_{сж}$ - об'єм стислого зображення-контейнера без вбудовування;

$W'_{сж}$ - об'єм стислого стеганографічного перетвореного зображення.

2.2 Оцінка проблемних недоліків існуючих методів стеганографічних перетворень

Проведемо аналіз ефективності існуючих стеганографічних методів. При цьому необхідно враховувати можливість застосування зловмисником активних і пасивних атак. Можливий спектр дій на стеганографічну систему, приведених в табл. 2.1, а саме атаки, направлені на:

- виявлення факту наявності вбудовування в зображенні спеціальної інформації;
- руйнування вбудованого повідомлення;
- вилучення (розкриття) вбудованого повідомлення.

Таблиця 2.1 -Спектр основних пасивних і активних атак на стеганографічну систему

	Мета здійснення атаки		
	Виявлення факту наявності вбудовування	Руйнування вбудованого повідомлення	Вилучення (розкриття) вбудованого повідомлення
Пасивні (неумисні)	Візуальна атака	Шуми в каналі передачі даних	-
Активні (навмисні)	За наявності апріорної інформації: - кореляційні методи. За відсутності апріорної інформації (стеганографічнийаналіз): - метод «хі-квадрат»; - RS-метод; - аналіз пар значень; - аналіз гістограм частот переходів; - аналіз числа переходів значень	Постановка завад. Компресійні атаки. Геометричні (афінні) атаки: - повороти; - масштабу-вання; - фрагментація. Фільтрація.	Стеганографічний аналіз

Для виявлення проблемних сторін існуючих підходів скритного вбудовування інформації, проведемо оцінку відносної стеганографічної ємкості $w_{отн}^{(m)}$ для наступних методів:

- метод вбудовування інформації в найменш значущий біт елемента спектрального представлення контейнера після квантування (режим 2 НЗБ);

- метод вбудовування інформації на основі розширення спектру (РС).

Розглянемо режим 2 для методу НЗБ. Цей режим передбачає безпосередню заміну біт двійкового представлення елементу спектрального представлення зображення-контейнера після квантування на значення біт приховуваної інформації.

У табл. 2.2 представлено значення відносної стеганографічної ємкості методів НЗБ в режимі 2 і РС для різних класів зображень. З аналізу значень в табл. 2.2 можна зробити висновок, що значення відносної стеганографічної ємкості для даних методів набуває значення від 0,78 до 6,25 %.

Таблиця 2.2 - Залежність значення $w_{отн}$ від ПВСШ для методів НЗБ і РС для різних класів зображень

Відносна ємкість %	Метод стеганографічного вбудовування		Значення ПВСШ, дБ		
			Сильно насичене зображення	Середньо насичене зображення	Слабо насичене зображення
6,25	НЗБ режим 2	$q=1$	14,67	14,12	14,62
		$q=2$	11,17	12,03	11,13
		$q=4$	8,69	9,11	8,79
3,1	НЗБ режим 2	$q=1$	32,12	33,42	31,43
		$q=2$	26,43	22,15	20,45
		$q=4$	18,54	18,27	18,03
0,78	РС	$\omega=16$	16,93	13,019	18,121

Тепер проведемо оцінку значення ймовірності $P_{из}$ безпомилкового вилучення вбудованих даних для методів вбудовування НЗБ і РС.

На рис. 2.1 представлені діаграми значень ймовірності $P_{из}$ безпомилкового вилучення вбудованих даних для методів НЗБ в режимі 2 і РС в умовах відсутності атак на вбудоване повідомлення.

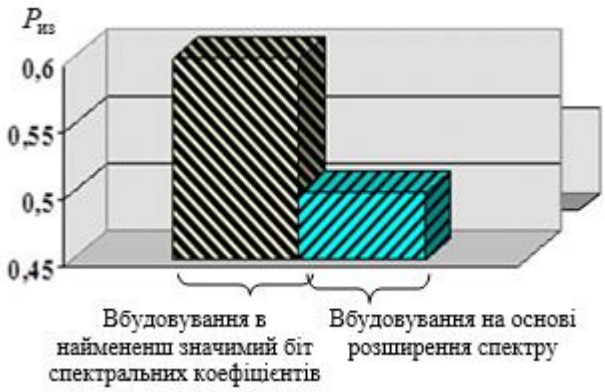

Рисунок 2.1 - Діаграма значень ймовірності $P_{из}$ для методів НЗБ в режимі 2, РС за умов відсутності атак на вбудоване повідомлення

З аналізу рис. 2.1 можна зробити висновки що:

- ймовірність безпомилкового вилучення вбудованих даних для методу НЗБ і РС може набувати значення від 0,5 до 0,6;

- для методу НЗБ в режимі 2 виграш відносно методу РС за значенням ймовірності безпомилкового вилучення вбудованих даних досягає рівня 0,1.

Проведемо оцінку ймовірності безпомилкового вилучення вбудованих даних в умовах атаки противника із застосуванням ДКП і квантування.

Заналізу рис. 2.2 можна зробити висновок, що для різних коефіцієнтів квантування кількість $w_{из}^{(m)}$ безпомилково вилучених біт для методів НЗБ в режимі 2 і РС приймає значення 50%.

Рисунок 2.2 - Порівняльна діаграма величини для методів НЗБ і РС в умовах атак зловмисника залежно від різних значень шагу квантування

З аналізу результатів досліджень існуючих стеганографічних систем можна зробити висновок, що методи безпосереднього стеганографічного вбудовування мають проблемні недоліки відносно значення стеганографічної ємності, пікового відношення сигнал-шум і ймовірності безпомилкового вилучення вбудованих даних [2].

Отже, існуючі методи стеганографічних перетворень не забезпечують повною мірою системних вимог по забезпеченню інформаційної безпеки в кризових ситуаціях з активним протистоянням противника.

2.3 Аспекти досліджень

Задоволення вимог до інформаційного забезпечення кризових систем пов'язане з підвищенням ефективності функціонування існуючих стеганографічних методів для прихованої передачі спеціальних інформаційних ресурсів. В цьому випадку для існуючих стеганографічних перетворень висуваються наступні вимоги:

1.Необхідність підвищення відносної стеганографічної ємності $w_{отн}$ методів вбудовування інформації. Дана вимога диктується постійним зростанням об'ємів і збільшенням змістовної значущості спеціальної інформації.

2. Необхідність підвищення ймовірності $P_{из}$ правильного вилучення вбудованих даних в умовах застосування активних атак. Наявність величезних можливостей зловмисника відносно реалізації атак, направлених на руйнування і модифікацію вбудованих даних. Це супроводжується підвищеними вимогами до стеганографічних методів відносно безпомилкового вилучення вбудованих даних.

3. Необхідність збільшення чинника візуальної стійкості стеганограми. Для забезпечення стійкості зображення з вбудованими даними до візуальних атак, направлених на встановлення факту наявності стеганографічного вбудовування.

Отже, в процесі використання існуючих стеганографічних методів для прихованої передачі спеціальної інформації виникає протиріччя, яке полягає в тому, що існуючі технології стеганографічних перетворень не забезпечують повною мірою нових системних вимог в кризових умовах за наявності дестабілізуючих чинників і протиборчих сторін.

Для вдосконалення існуючих і розробки нових методів стеганографічних перетворень необхідно використовувати принципово нові підходи, які повинні базуватися на сучасних і перспективних досягненнях в області теорії інформації, кодування, теорії обробки цифрових відеопросторів, технологій інтелектуального аналізу і методів криптографії. Одним з

актуальних напрямів є використання структурних перетворень елементів просторового представлення зображення для виявлення структурно-комбінаторної надлишковості. Такий підхід дозволить підвищити стійкість вбудованих даних до активних атак противника.

Звідси, напрям дослідження полягає в розробці теоретичних основ і методів підвищення безпеки спеціальної інформації на основі стеганографічного перетворення.

Структурно-комбінаторне стеганографічне кодування задається функціоналом $F\{P_{из}, w_{отн}, h\}$ в умовах виконання наступних обмежень:

$$\begin{cases} P_{из} \geq P_{из}^{(тр)}; \\ w_{отн} \geq w_{отн}^{(тр)}; \\ h \geq h^{(тр)}; \end{cases} \quad (2.8)$$

де $F\{P_{из}, w_{отн}, h\}$ - функціонал, який реалізує стеганографічний метод вбудовування спеціальної інформації;

$w_{отн}^{(тр)}$ - необхідне значення відносної стеганографічної ємкості системи;

$h^{(тр)}$ - необхідне значення пікового відношення сигнал-шум.

Таким чином, для досягнення поставленої необхідно вирішити наступні завдання:

- обґрунтувати підхід для вдосконалення методів безпосереднього вбудовування інформації в цифрове зображення-контейнер;

- розробити метод структурно-комбінаторного стеганографічного кодування для підвищення безпеки спеціальної інформації;

- створити метод для локалізації структурної стеганографічної надлишковості для підвищення стійкості відносно атак, направлених на виявлення факту вбудованої інформації;

- побудувати систему вбудовування інформації з маскуванням стеганографічної надлишковості.

3 МЕТОДОЛОГІЧНІ АСПЕКТИ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ БЕЗПОСЕРЕДНЬОГО СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ

3.1 Обгрунтування проблемних сторін функціонування технологій безпосереднього вбудовування

Безпосереднє вбудовування приховуваного повідомлення може здійснюватися як в просторово-часову, так і в просторово-частотну область зображення-контейнера. Як правило, таке вбудовування проводиться в окремий елемент поточного представлення зображення-контейнера (рис. 3.1), точніше в окремі біти елементу. В даному випадку елементом є двійкове позиційне число A_2 з основою, що дорівнює двом, тобто $A_2 = [A]_2$.

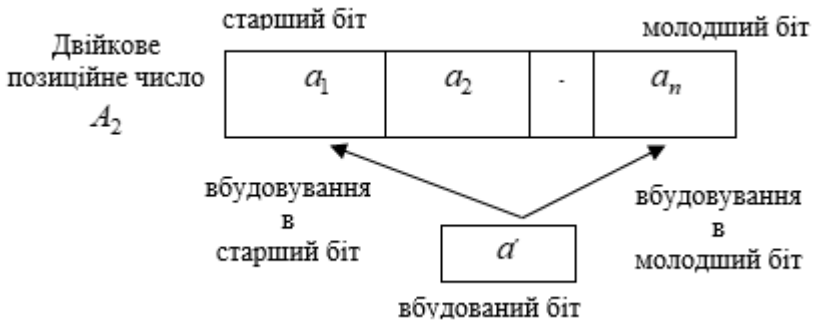

Рисунок 3.1 - Схема вбудовування біта приховуваного повідомлення в елемент поточного представлення зображення-контейнера

Процес безпосереднього вбудовування фактично є заміною одного біта вихідного елементу-контейнера на біт приховуваного повідомлення з використанням деякого функціонала φ_c, умови або правила [3].

У існуючих стеганографічних методах найбільш опрацьовані підходи, які ґрунтуються на вбудовуванні інформації в найменш значущі молодші (НЗБ) біти. У зв'язку з чим, розглянемо характеристики таких стеганосистем.

Метод вбудовування в найменш значущий біт здійснює заміну молодшого біта a_n двійкового позиційного числа A_2 на біт b_ξ вбудовуваного повідомлення B (рисунок 3.1). Це описується наступним виразом:

$$a'_n = b_\xi, \quad A'_2 = \{a_1, a_2, ..., a_{n\ 1}, a'_n\}, \tag{3.1}$$

де A'_2 - число, що містить вбудований біт a'_n приховуваного повідомлення.

Тут b_ξ - ξ-й елемент, вбудовуваної двійкової послідовності $B = \{b_1; ...; b_\xi; ...; b_\nu\}$, $a'_i \in [0;1]$; $b_\xi \in [0;1]$, $i = \overline{1, n}$; $\xi = \overline{1, \nu}$.

Узагальнено недоліки безпосереднього вбудовування біта приховуваного повідомлення в елемент-контейнер задаються наступним співвідношенням:

$$a'_\tau := \begin{cases} b_\xi \ \& \ P_{из}(b'_\xi = b_\xi) \to 0 \ \& \ \varepsilon(A; A') \to 0, \quad \tau \to n; \\ b_\xi \ \& \ P_{из}(b'_\xi = b_\xi) \to 1 \& \ \varepsilon(A; A') \to \max, \ \tau \to 1. \end{cases} \tag{3.2}$$

При вбудовуванні біта приховуваного повідомлення в старший біт вихідного числа спостерігається стійкість вбудованих даних при значних візуальних спотвореннях. І, навпаки, вбудовування в молодший біт характеризується низькою стійкістю вбудованих даних при мінімальних візуальних спотвореннях.

3.2 Обгрунтування підходу для побудови технології усунення недоліків безпосереднього стеганографічного вбудовування

Для усунення виявлених недоліків, тобто забезпечення візуальної стійкості стеганограми, при якій значення кількісної метрики $\varepsilon(A; A')$ буде найменшим, тобто

$$\varepsilon(A; A') \to 0 \tag{3.3}$$

і стійкості до трансформації і атак пропонується синтезувати функціонал $f(A')$ від *числа* з вбудованою інформацією.

3.3 Розробка технології функціонального перетворення чисел з імплантованими даними на основі нерівновагового позиційного кодування

В якості перетворювального функціонала, що характеризується властивостями у відповідності з вимогами відносно процесу приховання даних пропонується використовувати кодоутворювальну функцію для нерівновагового позиційного числа (НПЧ кодування), а як елемент-контейнер пропонується використовувати нерівновагове позиційне число [3].

В процесі нерівновагового позиційного кодування формуються кодові комбінації, що складаються з двох частин, а саме: інформаційна складова N і службова складова Ψ (рис. 3.2).

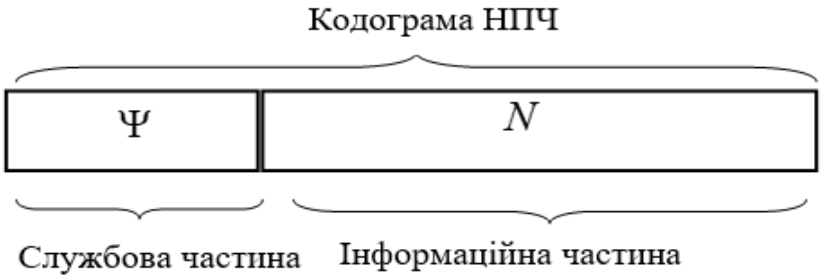

Рисунок 3.2 - Схема кодограми для нерівновагового позиційного числа

В цьому випадку вихідний елемент зображення розглядається як нерівновагове позиційне число A, яке складається з m елементів , а саме

$$A = \{a_{1,j}; ...; a_{i,j}; ...; a_{m,j}\}. \tag{3.4}$$

Для вихідного НП числа (рис. 3.3) A значення коду визначається за формулою:

$$N = f'(A), \tag{3.5}$$

де N - код вихідного нерівновагового позиційного числа A.

На другому етапі для сформованого значення коду N будується результуюче кодове представлення C_2 нерівновагового позиційного числа A:

$$C_2 = \varphi_c(N, \Psi). \tag{3.6}$$

Тут φ_c - оператор, що забезпечує побудову двійкової коду C_2 для кодового значення N і службових даних Ψ .

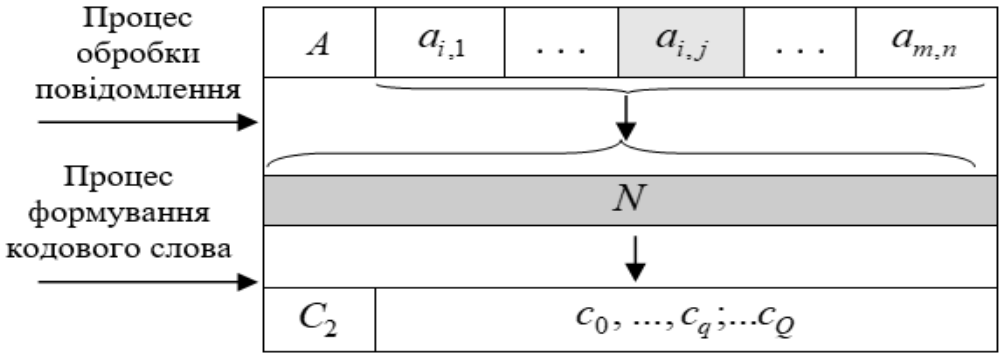

Рисунок 3.3 - Структурна схема побудови кодових конструкцій для нерівновагового позиційного числа А

В цьому випадку отримаємо

$$C_2 = \{c_1; \ldots; c_q; \ldots; c_Q\}; \quad c_q \in \{0; 1\}, \tag{3.7}$$

де Q - кількість біт на представлення НП числа C_2.

Службова складова включає інформацію про систему основ нерівновагового позиційного числа $\Psi = \{\psi_{i,j}\}$.

В разі такого підходу для формування кодового представлення C_2

нерівновагового позиційного числа A, оператор зворотнього функціонального перетворення $f^{(-1)'}(\bullet)$ дозволить отримати вихідне НП число A за наявності службової інформації Ψ. Вираз, який описує зворотнє функціональне перетворення має вигляд:

$$A = f^{(-1)'}(C_2; \Psi). \tag{3.8}$$

Для такого підходу принцип вбудовування пропонується вибирати таким чином (рис. 3.4).

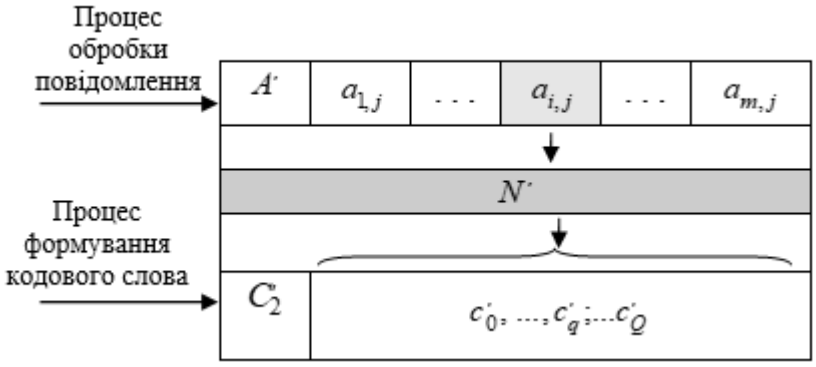

Рисунок 3.4 - Структурна схема побудови кодових конструкцій НП числа A' з вбудованими даними

У вихідне нерівновагове позиційне число A за допомогою оператора φ' вбудовується біт b_ξ приховуваного повідомлення B таким чином, що

$$A' = \varphi'(A; b_\xi). \tag{3.9}$$

Тут A' - нерівновагове позиційне число з вбудованим бітом b_ξ (НПЧ з вбудовуванням).

Після чого, визначається код N' для числа A':

$$N' = f'(A'). \tag{3.10}$$

На третьому етапі для сформованого значення коду N' будується результуюче кодове представлення C_2' нерівновагового позиційного числа A'

з вбудовуванням:

$$C_2' = \varphi_c(N', \Psi^{(1)}). \qquad (3.11)$$

Тут φ_c - оператор, що забезпечує побудову двійкового коду C_2'.

Зворотнє стеганографічне перетворення виконуватиметься за біполярним принципом для авторизованого (за наявності ключа $\Psi^{(2)}$) і неавторизованого користувача (зловмисника) за стандартних умов.

Перший спосіб використовується неавторизованим користувачем. Відновлення зображення відбувається за наявності відкритої службової інформації $\Psi^{(1)}$, що є системою основ НП числа A'. Таке зворотнє перетворення дозволяє достовірно реконструювати елемент $A''(1)$ по формулі:

$$A(1)'' = f'^{(-1)}(C_2; \Psi^{(1)}) \qquad (3.12)$$

так, щоб значення кількісної метрики $\varepsilon(A; A(1)'')$ було найменшим

$$\varepsilon(A; A(1)'') \to 0. \qquad (3.13)$$

Тут $A''(1)$ - елемент, реконструйований за стандартних умов.

Другий спосіб існує для авторизованого користувача. Тут зворотнє функціональне перетворення здійснюється з використанням відкритої службової інформації $\Psi^{(1)}$ і ключа $\Psi^{(2)}$. В даному випадку значення ключа $\Psi^{(2)}$ є заздалегідь відомим значенням основи вбудованого елементу так, щоб $\Psi^{(2)} \neq \Psi^{(1)}$. Зворотнє функціональне перетворення дозволить авторизованому користувачеві безпомилково реконструювати число з вбудованими даними, тобто:

$$A(2)'' = f'^{(1)}(C_2; \Psi^{(1)}; \Psi^{(2)}) \quad \text{і} \quad A(2)'' = A', \qquad (3.14)$$

де $A(2)''$ - нерівновагове позиційне число з вбудованими даними, отримане при зворотньому функціональному перетворенні авторизованим

користувачем.

Вилучення вбудованої інформації відбувається без внесення помилок внаслідок застосування оператора вилучення $\varphi_c'^{(1)}$ до нерівновагового позиційного числа $A(2)''$, що реконструюється, при якому також можливе безпомилкове відновлення числа A'' як елементу вихідного зображення:

$$\varphi'^{(-1)}(A''(2)) = \begin{cases} b'_\xi, & b'_\xi = b_\xi; \\ A''', & A''' = A. \end{cases} \tag{3.15}$$

Тут b'_ξ - вилучений елемент приховуваного повідомлення B'_2.

На рис. 3.5 представлена схема стеганографічного методу на основі нерівновагового позиційного кодування. Пряме стеганографічне перетворення реалізується в три етапи. На першому етапі за допомогою оператора вбудовування φ біт b_ξ приховуваного повідомлення B_2 вбудовується на різну позицію НП числа A. Отримане внаслідок завантаження біту b_ξ нерівновгове позиційне число A' визначається виразом

$$A' = \varphi(b_\xi; A). \tag{3.16}$$

На другому етапі для стеганочисла A' за правилом $f(A')$ формується код N', а саме:

$$N' = f'(A'). \tag{3.17}$$

Формування коду відбувається з врахуванням ключової інформації $\Psi^{(2)}$, що уявляє собою основу вбудованого елементу.

На третьому етапі будується результуюче кодове представлення C'_2 числа A' з вбудованими даними. Це описується виразом:

$$C'_2 = \varphi_c(N'; \Psi^{(1)}). \tag{3.18}$$

Отримана стеганограма C, що містить в собі інформаційну складову N' і службову складову $\Psi^{(1)}$, піддається атакуючим діям.

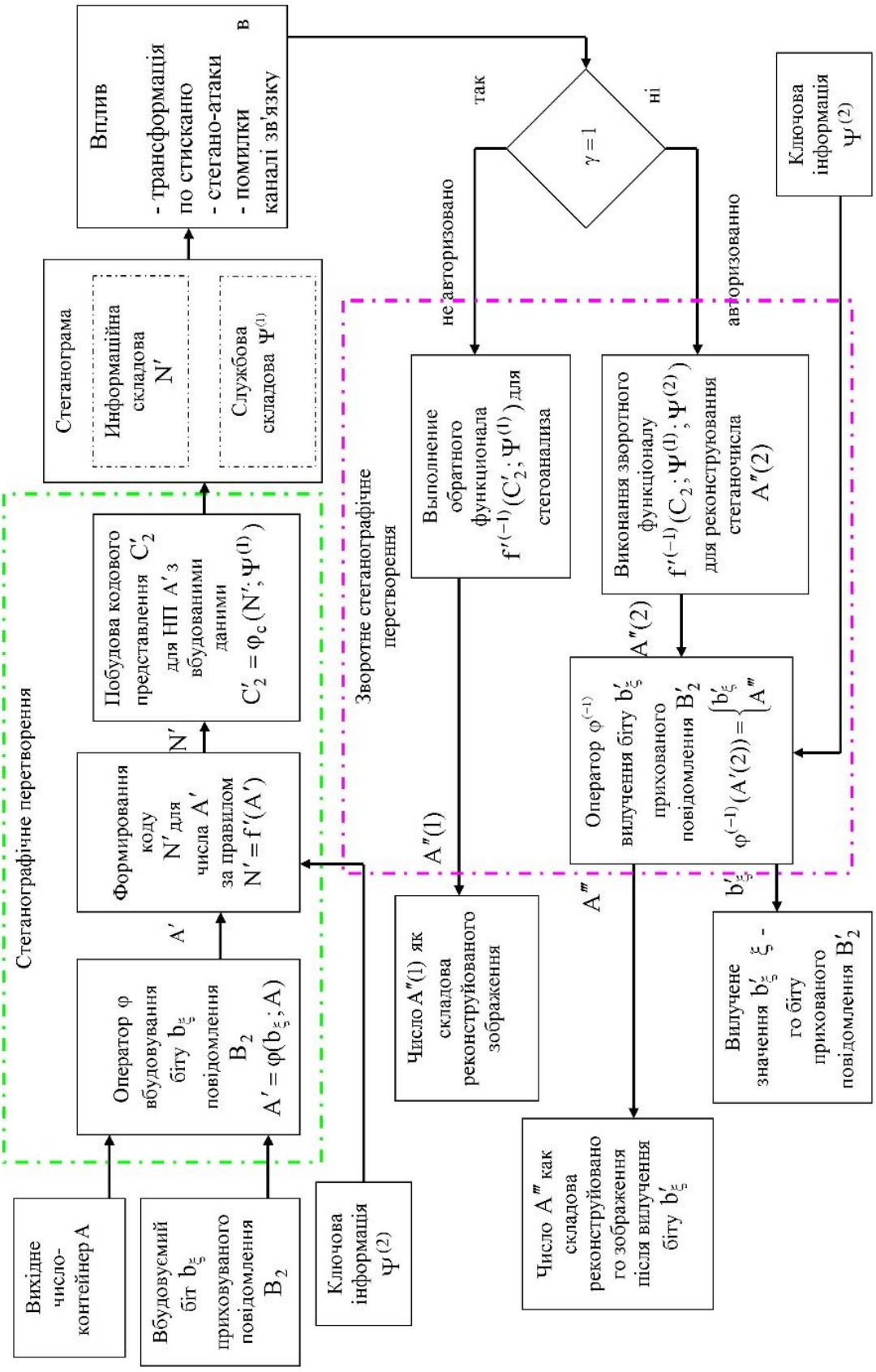

Рисунок 3.5 - Схема стеганографічного перетворення на основі нерівновагового позиційного кодування

Зворотнє стеганографічне перетворення включає випадок для неавторизованого користувача (стеганографічний аналіз) за умови, що йому відомий зворотній функціонал $f'^{(-1)}$. При стеганографічному аналізі, за правилом $f'^{(-1)}(\bullet)$ формується число, записуване як:

$$A''(1) = f'^{(-1)}(C_2'; \Psi^{(1)}). \tag{3.19}$$

Тут $A''(1)$- число, як складова зображення, що реконструюється, отримане в результаті стегоаналізу.

Для авторизованого користувача зворотнє стеганографічне перетворення відбувається в два етапи. На першому етапі за правилом $f'^{(-1)}(\bullet)$ і з врахуванням ключової інформації $\Psi^{(2)}$ відбувається реконструкція числа з вбудованими даними. Це задається таким співвідношенням:

$$A''(2) = f'^{(-1)}(C_2'; \Psi^{(1)}; \Psi^{(2)}). \tag{3.20}$$

На другому етапі з реконструйованого числа $A''(2)$ відбувається вилучення b_ξ' приховуваного повідомлення B_2. Внаслідок застосування оператора вилучення $\varphi'^{(1)}$ також відбувається реконструкція числа A''', як складового вихідного зображення, що описується виразом

$$\varphi'^{(1)}(A'(2)) = \begin{cases} b_\xi', & \Psi = \Psi^{(2)}; \\ A''', & \Psi = \Psi^{(2)}. \end{cases} \tag{3.21}$$

Таким чином, розроблений підхід для проектування стенографічної системи заснований на використанні функціонального перетворення для чисел з вбудованою інформацією.

4 МЕТОД СТРУКТУРНОГО СТЕГАНОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ КОРЕКЦІЇ НЕРІВНОВАГОВОГО ПОЗИЦІЙНОГО БАЗИСУ.

4.1 Обгрунтування проблемних сторін функціонування технологій маскування, шляхом відкидання молодшого біта кодограми

Імплантація одного біта $a'_{1,j}$ в старший елемент вихідного нерівноважного позиційного числа $A(j)$ в процесі стеганографічного кодування призводить до збільшення значення кодового представлення C'_j для стеганокода $N(j)'$. Тут утворюється кількість $R_{стег}$ стеганографічної надмірності. Локалізація стеганографічної надмірності полягає в відкиданні молодшого біта кодограми C'_j стеганокода $N(j)'$ за правилом:

$$N(j)''' = N(j)' / 2 \; ; C'''_j = \{c_1, ..., c_\tau, ..., c_{q(j)'-1}\}.$$

тут $N(j)'''$ - значення скоригованого стеганокода; C'''_j - кодограмм скоригованого стеганокода $N(j)'''$.

Однак, таке коригування призводить до виникнення залишкових спотворень в разі реконструкції зображення зловмисником. Це відбувається в результаті того, що:

а) з одного боку для зловмисника відновлення елемента $a'''_{i,j}$ нерівновагового позиційного числа здійснюється для скоригованого значення стеганокода $N(j)'''$. Для цього використовується формула

$$a'''_{i,j} = [\, N(j)''' / V_{i,j} \,] - [\, N(j)''' / (\psi_{i,j} V_{i,j}) \,] \, \psi_{i,j}; \qquad (4.1)$$

б) з іншого боку для заданої системи основ нерівновагового позиційного базису відновити вихідні елементи нерівновагового позиційного числа можливо тільки для значення коду-контейнера $N(j)$.

Тому для зловмисника значення реконструйованих елементів $a'''_{i,j}$ можуть відрізнятися від значень вихідних елементів $a_{i,j}$, Тобто

$$a'''_{i,j} \neq a_{i,j} .$$

Приклади зображень «Знімок аеропорту» і «Лена», декодованих при неавторизований доступ (Додаток А.1, А.2). Для таких зображень спостерігається поява великої кількості візуальних спотворень. У той же час кількісна оцінка якості реконструйованих зображень на основі значення пікового відношення сигнал-шум показує, що найкраща якість забезпечується для сильнонасичених зображень в порівнянні з средньонасиченими зображеннями [4]. Значення пікового відношення сигнал-шум для реконструйованого сильнонасиченого зображення «Знімок аеропорту» і средньонасичене зображення «Лена» щодо вихідних зображень рівні відповідно 17 дБ і 13 дБ.

У той же час, розглянута локалізація структурою стеганографічної надмірності проявляється також і в разі стеганографічного декодування зображення авторизованим користувачем.

У цьому випадку механізм демаскування полягає в додаванні молодшого нульового біта до двійкового змістом стеганокода $N(j)'''$. Таке перетворення задається наступною формулою:

$$N(j)^{*} = N(j)''' \cdot 2, C'''_j = \{C'_j; 0\} = \{c_1, ..., c_\tau, ..., c_{q(j)'-1}, 0\},$$

де $N(j)^*$- значення демаскувати стеганокода в разі авторизованого користувача.

Однак, дана дія не завжди буде призводити до отримання початкового значення стеганокода $N(j)'$. Можливі випадки, коли значення скоригованого стеганокода $N(j)^*$ буде відрізнятися від вихідного значення стеганокода $N(j)'$ значенням молодшого біта, тобто

$$c'_{q(j)'} \neq c^*_{q(j)'} = 0.$$

Звідки виконується нерівність:

$$N(j)^* \neq N(j)'.$$

Відповідно це створює умова для того, що не всі елементи відновленого нерівновагового позиційного числа $A(j)^*$ збігатимуться з елементами вихідного нерівноважного позиційного числа $A(j)$, Тобто

$$a^*_{i,j} \neq a_{i,j}\ , \ i = \overline{i,m}.$$

Звідси можна зробити висновок, що запропонований метод локалізації стеганографічної надмірності в умовах стеганографічного кодування всіх нерівноважних позиційних чисел обмеженої довжини:

- знижує ефективність приховування вбудовується інформації;
- знижує якість вихідних зображень.

У зображеннях, отриманих в результаті стеганографічного декодування для авторизованого користувача, спостерігається поява незначного кількість імпульсних помилок. При цьому кількісна оцінка якості стеганографічно декодованих зображень на основі значення пікового

відношення сигнал-шум показало, що найкращу якість забезпечується для сильнонасичених зображень в порівнянні з середньонасиченими зображеннями. Значення пікового відношення сигнал-шум для реконструйованого сыльнонасиченого зображення «Знімок аеропорту» і середньносиченого зображення «Лена» щодо вихідних зображень рівні відповідно 27 дБ і 22 дБ.

4.2 Обгрунтування методу структурного стеганографічного кодування на основі корекції нерівновагового позиційного базису

Отже, необхідно розробити підхід для локалізації структурної стеганографічної надмірності, реалізація якого не пов'язана з корекцією стеганокода.

При цьому обов'язковою умовою є забезпечення відповідності меду довжиною $q(j)'$ кодограми стеганокода $N(j)'$ і довжиною $q(j)$ коду-контейнера $N(j)$ в разі неавторизованого доступу до стеганографічно перетвореному зображенню.

Для цього пропонується організувати локалізацію структурної стеганографічної надмірності на основі побудови модифікованої системи основ $\Psi'^{(1)}$. Під модифікацією системи основ розуміється корекція значень окремих основ.

Обгрунтування даного підходу полягає в тому, що довжина $q(j)$ кодограми як для кода- контейнера $N(j)$, Так і для стеганокода $N(j)'$ визначається відповідно на основі накопиченого твори основ, тобто

$$q(j) = \log_2 \prod_{i=1}^{m} \psi_{i,j} ;$$

$$q(j)' = \log_2((\prod_{i=1}^{\gamma-1} \psi_{i,j}) \cdot \psi'_{\gamma,j} \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j}).$$

Тому за рахунок корекції окремих основ досягається можливість вирівняти довжину $q(j)'$ стеганокода $N(j)'$ і довжину $q(j)$ коду-контейнера $N(j)$. В цьому випадку виконується співвідношення:

$$q(j)'' = \log_2((\prod_{i=1}^{\eta-1} \psi_{i,j}) \cdot \psi''_{\eta,j} \cdot \prod_{i=\eta+1}^{m} \psi_{i,j}) = \log_2(2 \cdot \prod_{i=1}^{m} \psi_{i,j}) = q(j)',$$

де $\psi''_{\eta,j}$- модифіковане основу η-го елемента нерівновагового позиційного числа $A(j)$ вихідної відео послідовності.

Оскільки в нерівновагове позиційне число імплантується тільки один елемент приховуваного повідомлення, то досить корекції тільки одного основи [4]. Хоча в загальному випадку можлива одночасна корекція основ кількох елементів. Корекція основи повинна проводиться з урахуванням того, що основа вбудованого елемента дорівнює двом, $\psi'_{\gamma,j} = 2$. Значить, і довжина $q(j)'$ кодового представлення стеганокода $N(j)'$ буде більше довжини $q(j)$ кодограми коду-контейнера на один біт. Тому для корекції досить змінити основу одного елемента. Корекцію основи пропонується проводити на базі наступного умови:

$$q(j)'' = q(j)'$$

або

$$q(j)'' = \log_2((\prod_{i=1}^{\eta-1} \psi_{i,j}) \cdot \psi''_{\eta,j} \cdot \prod_{i=\eta+1}^{m} \psi_{i,j} = \log_2(2 \cdot \prod_{i=1}^{m} \psi_{i,j}) = q(j)'.$$

Для скорочення кількості операцій пропонується використовуватися правило, заданий формулою:

$$\psi''_{\eta,j} = 2 \cdot \psi_{\eta,j},$$

де $\psi_{\eta,j}$- основа η-го елемента нерівновагового позиційного числа A(j) вихідної відео послідовності.

Розглянемо варіанти вибору позиції елемента нерівновагового позиційного числа, для якого будемо проводити коригування основи. На вибір такої позиції впливає те, що необхідно забезпечити наступні вимоги:

а) забезпечити умова безпогрешного вилучення вбудованої інформації;

б) забезпечити мінімізацію спотворень зображення, реконструйованого як для авторизованого, так і для неавторизованого користувача.

Для реалізації першої умови сформулюємо і доведемо наступну теорему.

Теорема 4.1. (Умова безпогрешного вилучення вбудованої інформації). Для реалізації першого напрямку корекційна основу $\psi''_{\eta,j}$ має відповідати елементу НП числа, що займає більш старшу позицію η в порівнянні з позицією γ вбудованого елемента $a'_{\gamma,j}$, Тобто

$$a'_{\gamma,j} = a''_{\gamma,j}, \text{ коли } \psi''_{\eta,j} | \eta > \gamma. \qquad (4.2)$$

Доведемо це. Доказ будемо проводити від противного. У зв'язку з чим виберемо позицію елемента з корекційною основою η меншим, ніж позиція γ вбудованого елемента, тобто:

$$\gamma > \eta .$$

В цьому випадку ваговий коефіцієнт $V'_{\gamma,j}$ вбудованого елемента $a'_{\gamma,j}$ буде обчислюватися за формулою:

$$V'_{\gamma,j} = \prod_{i=\gamma+1}^{m+1} \psi_{i,j} .$$

При вилученні вбудованого елемента $a''_{\gamma,j}$, його ваговий коефіцієнт $V''_{\gamma,j}$ буде обчислюватися з урахуванням модифікованого основи $\psi''_{\eta,j}$ на основі виразу

$$V''_{\gamma,j} = (\prod_{i=\gamma+1}^{\eta-1} \psi_{i,j}) \cdot \psi''_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j} .$$

Беручи до уваги те, що

$$\psi''_{\eta,j} = k \cdot \psi_{\eta,j}$$

отримаємо такий вираз:

$$V''_{\gamma,j} = (\prod_{i=\gamma+1}^{\eta-1} \psi_{i,j}) \cdot (k \cdot \psi_{\eta,j}) \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j} = k \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j} \neq V'_{\gamma,j} , \qquad (4.3)$$

де k - коефіцієнт модифікації основи $\psi_{\eta,j}$, $k > 1$.

Припустимо, що $\eta = \gamma + 1$. Звідси значення вилученого вбудованого елемента $a''_{\gamma,j}$ буде обчислюватися з урахуванням вагового коефіцієнта $V''_{\gamma,j}$ на основі виразу:

$$a''_{\gamma,j} = [\,N(j)'/V''_{\gamma,j}\,] - [\,N(j)'/(\psi'_{\gamma,j}\,V''_{\gamma,j})\,]\,\psi'_{\gamma,j}\ .$$

Розпишемо цей вислів з урахуванням співвідношення для:

$$N(j)' = \sum_{i=1}^{\gamma} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}.$$

Тоді отримаємо:

$$a''_{\gamma,j} = [(\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j})/V''_{\gamma,j}] -$$

$$-[(\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j})/(\psi'_{\gamma,j} V''_{\gamma,j})]\cdot\psi'_{\gamma,j} =$$

$$= [\ \frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}}\ ] -$$

$$-[\ \frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}}\ ]\cdot\psi'_{\gamma,j}\ . \qquad (4.4)$$

Тепер розглянемо перший доданок правої частини виразу (4.4):

$$[\ \frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}}\ ]\ . \qquad (4.5)$$

Третє складова в вираженні (4.5) з огляду на наступні нерівності:

$$V''_{\gamma,j} = k \cdot V'_{\gamma,j} > V'_{\gamma,j};\ V'_{\gamma,j} > \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j} \qquad (4.6)$$

буде приймати значення менше одиниці, тобто

$$\frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} < 1$$

або

$$\frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} = 0.$$

В цьому випадку вираз (4.4) Набуде вигляду:

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} \right].$$

Основами в отриманий вираз формулу для вагового коефіцієнта вбудованого елемента $V''_{\gamma,j}$:

$$V''_{\gamma,j} = k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}, \text{ для } \eta = \gamma + 1.$$

тоді отримаємо

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}}\right] = \left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}}\right].$$

Тепер перепишемо отримане вираження з урахуванням наступних співвідношення для вагових коефіцієнтів $V'_{\gamma,j}$ і $V'_{i,j}$:

$$V'_{\gamma,j} = \prod_{i=\gamma+1}^{m+1} \psi_{i,j} = \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j} \ ;$$

$$V'_{i,j} = \prod_{\xi=i+1}^{\gamma} \psi_{\xi,j} \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j} \text{, для} \eta = \gamma + 1. \qquad (4.7)$$

Тоді перший доданок правої частини виразу (4.4) набуде вигляду:

$$\left[\frac{\sum_{i=1}^{\gamma-1} a_{i,j} \cdot \prod_{\xi=i+1}^{\gamma} \psi_{\xi,j} \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}}{k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}} + \frac{a'_{\gamma,j} \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}}{k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}}\right] =$$

$$= \left[\frac{\sum_{i=1}^{\gamma-1} a_{i,j} \cdot \prod_{\xi=i+1}^{\gamma} \psi_{\xi,j}}{k} + \frac{a'_{\gamma,j}}{k}\right].$$

Тепер перетворимо другий доданок правої частини виразу (4.4):

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}}\right] \cdot \psi'_{\gamma,j}. \qquad (4.8)$$

При цьому будемо враховувати наступні співвідношення:

$$V''_{\gamma,j} = k \cdot V'_{\gamma,j} > V'_{\gamma,j}; \psi'_{\gamma,j} V''_{\gamma,j} > \sum_{i=\gamma}^{m+1} a_{i,j} V_{i,j}.$$

Тоді друге і третє доданок вираження (4.8) Прийме значення менше одиниці, тобто

$$\frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} < 1; \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} < 1$$

або

$$\frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} = 0; \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} = 0.$$

У цьому випадку другий доданок правої частини виразу (4.4) Прийме наступний вигляд:

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} \right] \cdot \psi'_{\gamma,j} = \left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} \right] \cdot \psi'_{\gamma,j}.$$

Основні, в отриманому виразі, наступні співвідношення для вагових коефіцієнтів $V''_{\gamma,j}$ і $V'_{i,j}$:

$$V''_{\gamma,j} = k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j} \ , \ \eta = \gamma + 1,$$

$$V'_{i,j} = \prod_{\xi=i+1}^{\gamma-1} \psi_{\xi,j} \cdot \psi'_{\gamma,j} \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j} \cdot$$

Тоді отримаємо:

$$\left[\frac{\sum_{i=1}^{\gamma-1} a_{i,j} \cdot \left(\prod_{\xi=i+1}^{\gamma-1} \psi_{\xi,j} \right) \cdot \psi'_{\gamma,j} \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}}{\psi'_{\gamma,j} \cdot k \cdot \psi_{\eta,j} \cdot \prod_{i=\eta+1}^{m+1} \psi_{i,j}} \right] \cdot \psi'_{\gamma,j} = \left[\frac{\sum_{i=1}^{\gamma-1} a_{i,j} \cdot \left(\prod_{\xi=i+1}^{\gamma-1} \psi_{\xi,j} \right)}{k} \right] \cdot \psi'_{\gamma,j} \cdot$$

Запишемо вираз (4.4) з урахуванням перетвореного першого і другого доданків правої частини. В цьому випадку отримаємо:

$$a''_{\gamma,j} = \left[\frac{\sum_{i=1}^{\gamma-1} a_{i,j} \cdot \left(\prod_{\xi=i+1}^{\gamma-1} \psi_{\xi,j} \right) \cdot \psi'_{\gamma,j}}{k} + \frac{a'_{\gamma,j}}{k} \right] - \left[\frac{\sum_{i=1}^{\gamma-1} a_{i,j} \cdot \prod_{\xi=i+1}^{\gamma-1} \psi_{\xi,j}}{k} \right] \cdot \psi'_{\gamma,j} \cdot$$

Звідки можна зробити висновок, що $a''_{i,j} = a'_{\gamma,j}$, в разі коли $k = 1$. Однак умови маскування структурної стеганографічної надмірності передбачає, що коефіцієнт модифікації основи приймає значення більше одного, тобто $k > 1$. Отже, в загальному випадку:

$$a''_{i,j} \neq a'_{\gamma,j} .$$

З іншого боку, коли $\gamma < \eta$, значення $V'_{\gamma,j}$ вилученого елемента $a''_{\gamma,j}$ буде визначатися без урахування модифікованого основи $\psi''_{\eta,j}$ за формулою:

$$V''_{\gamma,j} = \prod_{i=\gamma+1}^{m+1} \psi_{i,j} = V'_{\gamma,j} \quad . \tag{4.9}$$

Припустимо, що $\eta = \gamma - 1$. У цьому випадку значення $a''_{\gamma,j}$ буде визначатися без похибки за формулою:

$$a''_{\gamma,j} = [\,N(j)'/V''_{\gamma,j}\,] - [\,N(j)'/(\psi'_{\gamma,j}\,V''_{\gamma,j})\,]\,\psi'_{\gamma,j}\ .$$

Розпишемо цей вислів з урахуванням співвідношення для:

$$N(j)' = \sum_{i=1}^{\gamma} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}.$$

Тоді отримаємо:

$$a''_{\gamma,j} = [(\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}) / V''_{\gamma,j}] -$$

$$- [(\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}) / (\psi'_{\gamma,j} V''_{\gamma,j})] \cdot \psi'_{\gamma,j} =$$

$$= [\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}}] -$$

$$- [\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}}] \cdot \psi'_{\gamma,j} \quad . \tag{4.10}$$

Розглянемо перший доданок правої частини виразу (4.10):

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}}\right]. \qquad (4.11)$$

перетворимо вираз (4.11) З урахуванням наступного нерівності:

$$V''_{\gamma,j} = V'_{\gamma,j} > \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}. \qquad (4.12)$$

У цьому випадку другий доданок виразу (4.12) набуде вигляду:

$$\frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} = \frac{a'_{\gamma,j} V'_{\gamma,j}}{V'_{\gamma,j}} = a'_{\gamma,j},$$

а третій доданок прийме значення менше одиниці, тобто

$$\frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} < 1.$$

Тоді вираз (4.11) Прийме наступний вигляд:

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{V''_{\gamma,j}}\right] = \left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{V'_{\gamma,j}} + a'_{\gamma,j}\right].$$

Перетворимо дане вираження, з огляду на наступні співвідношення для вагових коефіцієнтів $V'_{\gamma,j}$ і $V'_{i,j}$:

$$V'_{\gamma,j} = \prod_{i=\gamma+1}^{m+1} \psi_{i,j} \ , \ V'_{i,j} = \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} \cdot \psi'_{\gamma,j} \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j} \ , \text{ де } \eta = \gamma - 1.$$

У цьому випадку перший доданок правої частини частину виразу (4.10) Набуде вигляду:

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} \cdot \psi'_{\gamma,j} \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j}}{\prod_{i=\gamma+1}^{m+1} \psi_{i,j}} + a'_{\gamma,j} \right] = \sum_{i=1}^{\gamma} a_{i,j} \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} \cdot \psi'_{\gamma,j} + a'_{\gamma,j} \ .$$

Тепер розглянемо другий доданок вираження (4.10):

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} \right] \cdot \psi'_{\gamma,j}. \qquad (4.13)$$

З огляду на наступне нерівність

$$V''_{\gamma,j} = V'_{\gamma,j} > \sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}$$

третій доданок вираження (4.13) Прийме значення менше одиниці, тобто:

$$\frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} < 1.$$

Перетворимо другий доданок вираження (4.13) З урахуванням нерівності:

$$\psi'_{\gamma,j} V''_{\gamma,j} = \psi'_{\gamma,j} V'_{\gamma,j} > a'_{\gamma,j} V'_{\gamma,j}.$$

В цьому випадку доданок також прийме значення менше одиниці, тобто:

$$\frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} < 1.$$

Тоді вираз (4.13) набуде вигляду:

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{a'_{\gamma,j} V'_{\gamma,j}}{\psi'_{\gamma,j} V''_{\gamma,j}} + \frac{\sum_{i=\gamma+1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}}\right] \cdot \psi'_{\gamma,j} = \left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}}\right] \cdot \psi'_{\gamma,j}.$$

Перетворимо дане вираження, з огляду на таке співвідношення для вагових коефіцієнтів $V'_{i,j}$ і $V''_{\gamma,j}$:

$$V''_{\gamma,j} = V'_{\gamma,j} = \prod_{i=\gamma+1}^{m+1} \psi_{i,j}, \; V'_{i,j} = \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} \cdot \psi'_{\gamma,j} \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j}, \text{ де } \eta = \gamma - 1.$$

У цьому випадку другий доданок вираження (4.10) Прийме наступний вигляд:

$$\left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V''_{\gamma,j}}\right] \cdot \psi'_{\gamma,j} = \left[\frac{\sum_{i=1}^{\gamma} a_{i,j} V'_{i,j}}{\psi'_{\gamma,j} V'_{\gamma,j}}\right] \cdot \psi'_{\gamma,j} =$$

$$= \left[\frac{\sum_{i=1}^{\gamma} a_{i,j} \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} \cdot \psi'_{\gamma,j} \cdot \prod_{i=\gamma+1}^{m+1} \psi_{i,j}}{\psi'_{\gamma,j} \prod_{i=\gamma+1}^{m+1} \psi_{i,j}}\right] \cdot \psi'_{\gamma,j} = \sum_{i=1}^{\gamma} a_{i,j} \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} .$$

перепишемо вираз (4.10) з урахуванням перетвореного першого і другого доданків:

$$a''_{\gamma,j} = \sum_{i=1}^{\gamma} a_{i,j} \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} \cdot \psi'_{\gamma,j} + a'_{\gamma,j} - \sum_{i=1}^{\gamma} a_{i,j} \prod_{\xi=i+1}^{\eta} \psi_{\xi,j} = a'_{\gamma,j} .$$

Звідки можна зробити висновок, що

$$a''_{\gamma,j} = a'_{\gamma,j}.$$

Іншими словами, вилучення вбудованого елемента $a''_{\gamma,j}$ здійснюється без помилки в разі, коли позиція γ вбудованого елемента молодше позиції η елемента з модифікованим основою, тобто $\gamma < \eta$.

Теорема доведена.

Розглянемо другу вимогу, коли вибір позиції вбудовування елемента $a'_{\gamma,j}$ повинен забезпечити мінімізацію внесених спотворень при реконструкції елементів $a'''_{i,j}$ вихідної відеопослідовності. Як показник мінімізації спотворень пропонується використовувати умова, що складається в мінімізації різниці між значенням коду-контейнера N(j) і стеганокодом N(j)′. Для цього використовується наступне співвідношення:

$$\Delta N(j) = N(j)' - N(j),$$

де $\Delta N(j)$ - значення пульсації стеганокода.

У разі імплантації елемента $a'_{\gamma,j}$ на γ-у позицію нерівновагового позиційного числа $A(j)$ значення стеганокода $N(j)'$ для НПЧ $A(j)'$ з імплантацією буде обчислюватися на основі наступного виразу:

$$N(j)' = \sum_{i=1}^{\gamma-1} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma+1}^{m+1} a_{i,j} \overline{V}_{i,j},$$

де $\overline{V}_{i,j}$ - ваговий коефіцієнт елемента $a_{i,j}$ при $i > \gamma$.

Перетворимо третій доданок цього виразу з урахуванням наступного нерівності:

$$\overline{V}_{i,j} = V_{i-1,j},\ i = \overline{\gamma+1,\ m+1}.$$

В цьому випадку доданок прийме наступний вигляд:

$$\sum_{i=\gamma+1}^{m+1} a_{i,j} \overline{V}_{i,j} = \sum_{i=\gamma}^{m} a_{i,j} V_{i,j}. \qquad (4.14)$$

Перепишемо формулу для стеганокода $N(j)'$ з урахуванням виразу (4.14). В цьому випадку отримаємо:

$$N(j)' = \sum_{i=1}^{\gamma-1} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma}^{m} a_{i,j} V_{i,j}.$$

Значення коду-контейнера $N(j)$ визначається на основі наступної формули:

$$N(j) = \sum_{i=1}^{m} a_{i,j} V_{i,j} .$$

Тоді значення величини $\Delta N(j)$ обчислюється за формулою:

$$\Delta N(j) = N(j)' - N(j) =$$

$$= (\sum_{i=1}^{\gamma-1} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=\gamma}^{m} a_{i,j} V_{i,j}) - (\sum_{i=1}^{m} a_{i,j} V_{i,j}) =$$

$$= \sum_{i=1}^{\gamma-1} a_{i,j} V'_{i,j} + a'_{\gamma,j} V'_{\gamma,j} + \sum_{i=1}^{\gamma-1} a_{i,j} V_{i,j} =$$

$$= \sum_{i=1}^{\gamma-1} a_{i,j} (V'_{i,j} - V_{i,j}) + a'_{\gamma,j} V'_{\gamma,j} . \qquad (4.15)$$

Перепишемо вираз (4.15) з урахуванням наступного співвідношення для вагового коефіцієнта $V'_{i,j}$:

$$V'_{i,j} = \psi'_{\gamma,j} \cdot V_{i,j}.$$

В цьому випадку отримаємо:

$$\Delta N(j) = \sum_{i=1}^{\gamma-1} a_{i,j} (V'_{i,j} - V_{i,j}) + a'_{\gamma,j} V'_{\gamma,j} = \sum_{i=1}^{\gamma-1} a_{i,j} (\psi'_{\gamma,j} V_{i,j} - V_{i,j}) + a'_{\gamma,j} V'_{\gamma,j} =$$

$$= (\sum_{i=1}^{\gamma-1} a_{i,j} V_{i,j} (\psi'_{\gamma,j} - 1)) + a'_{\gamma,j} V'_{\gamma,j} .$$

З огляду на те, що значення вбудованого елемента приймає значення $a'_{\gamma,j} = [\,0; 1\,]$, а його основу $\psi'_{\gamma,j}$ вибрано мінімально можливим і одно $\psi'_{\gamma,j} = 2$, отриманий вираз прийме наступний вигляд:

$$\Delta N(j) = \begin{cases} \sum_{i=1}^{\gamma-1} a_{i,j} V_{i,j}\,, & \to a'_{\gamma,j} = 0; \\ \sum_{i=1}^{\gamma-1} a_{i,j} V_{i,j} + V'_{\gamma,j}\,, & \to a'_{\gamma,j} = 1. \end{cases}$$

тоді величина $\Delta N(j)$ буде прагнути до нульового значення в разі, коли позиція вбудованого елемента γ буде приймати мінімальні значення, тобто:

$$\gamma \to \min.$$

Значить, можна зробити висновок, що для запропонованого механізму локалізації структурної стеганографічної надмірності коректовані основа повинна відповідати елементу нерівновагового позиційного числа на більш старшої позиції в порівнянні з позицією вбудованого елемента.

У той же час для забезпечення стійкості вбудованої інформації до стегоатакам необхідно щоб значення вагового коефіцієнта вбудованого елемента було найбільшим. З огляду на цей факт пропонується будувати правило маскування стеганографічної надмірності на основі наступних принципів:

а) вбудовувати елемент $a'_{\gamma,j}$ приховуваного повідомлення на другу позицію $\gamma = 2$ в нерівноваговому позиційному числі;

б) піддавати корекції основі першого елемента НП числа.

Дане правило забезпечує:

1. Вирівнювання довжини $q(j)$ кодограми коду-контейнера щодо довжини $q(j)'$ кодограми стеганокода $N(j)'$. Це описується формулою:

$$q(j) = \log_2(\psi''_{1,j} \cdot \prod_{i=2}^{m} \psi_{i,j}) = \log_2(2 \cdot \psi_{1,j} \cdot \prod_{i=2}^{m} \psi_{i,j}) = \log_2 2 \cdot \prod_{i=1}^{m} \psi_{i,j} = q(j)'.$$

Це дозволить маскувати для зловмисника факт наявності вбудовування інформації. Іншими словами, на основі модифікованої системи основ зловмисник правильно визначає довжину $q(j)'$ стеганокода.

2. У разі авторизованого доступу відновлення елемента приховуваного повідомлення здійснюється без втрат. Для цього розглянемо процес реконструкції вбудованого елемента $a''_{2,j}$ за формулою:

$$a''_{2,j} = [N(j)'/V'_{2,j}] - [N(j)'/(\psi'_{2,j} V'_{2,j})]\,\psi'_{2,j}.$$

Розпишемо цей вислів з урахуванням формули для стеганокода:

$$N(j)' = a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}.$$

Тоді отримаємо:

$$a''_{2,j} = [(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j})/V'_{2,j}] -$$

$$-[(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j})/(\psi'_{2,j}V'_{2,j})]\cdot\psi'_{2,j} =$$

$$= [\frac{a_{1,j}V'_{1,j}}{V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{2,j}}] -$$

$$-[\frac{a_{1,j}V'_{1,j}}{\psi'_{2,j}V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi'_{2,j}V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi'_{2,j}V'_{2,j}}]\cdot\psi'_{2,j}, \qquad (4.16)$$

де $a'_{2,j}$- біт приховуваного повідомлення, імплантований на позицію $\gamma = 2$ другого елемента нерівновагового позиційного числа;

$a''_{2,j}$ - відновлений біт приховуваного повідомлення для авторизованого користувача.

Розглянемо перший доданок правої частини виразу (4.16):

$$[\frac{a_{1,j}V'_{1,j}}{V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{2,j}}]. \qquad (4.17)$$

Перетворимо вираження (4.17) з урахуванням наступного нерівності:

$$V'_{2,j} > \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}.$$

Тоді третій доданок вираження (4.17) прийме значення менше одиниці, тобто:

$$\frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{2,j}} < 1.$$

Другий доданок вираження прийме вигляд:

$$\frac{a'_{2,j}V'_{2,j}}{V'_{2,j}} = a'_{2,j}.$$

перепишемо вираз (4.17) з урахуванням отриманих перетворень. В цьому випадку отримаємо:

$$[\frac{a_{1,j}V'_{1,j}}{V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{2,j}}] = [\frac{a_{1,j}V'_{1,j}}{V'_{2,j}} + a'_{2,j}].$$

Перетворимо дане вираження, з огляду на таке співвідношення для вагових коефіцієнтів $V'_{1,j}$ і $V'_{2,j}$:

$$V'_{2,j} = \prod_{i=3}^{m+1} \psi_{i,j} \; ; V'_{1,j} = \psi'_{2,j} \cdot \prod_{i=3}^{m+1} \psi_{i,j}.$$

В цьому випадку отримаємо:

$$[\frac{a_{1,j}V'_{1,j}}{V'_{2,j}} + a'_{2,j}] = [\frac{a_{1,j} \cdot \psi'_{2,j} \cdot \prod_{i=3}^{m+1} \psi_{i,j}}{\prod_{i=3}^{m+1} \psi_{i,j}} + a'_{2,j}] = a_{1,j} \cdot \psi'_{2,j} + a'_{2,j}.$$

Тепер розглянемо другий доданок правої частини виразу (4.16):

$$[\frac{a_{1,j}V'_{1,j}}{\psi'_{2,j}V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi'_{2,j}V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi'_{2,j}V'_{2,j}}] \cdot \psi'_{2,j}. \qquad (4.18)$$

Перетворимо вираз (4.18) з урахуванням наступного нерівності:

$$\psi'_{2,j} V'_{2,j} > a'_{2,j} V'_{2,j}.$$

В цьому випадку другий і третій доданки виразу (4.18) прийматимуть значення менше одиниці, тобто:

$$\frac{a'_{2,j} V'_{2,j}}{\psi'_{2,j} V'_{2,j}} < 1; \frac{\sum_{i=3}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{2,j} V'_{2,j}} < 1.$$

Перепишемо другий доданок вираження (4.16) з урахуванням виконаних перетворень:

$$[\frac{a_{1,j} V'_{1,j}}{\psi'_{2,j} V'_{2,j}} + \frac{a'_{2,j} V'_{2,j}}{\psi'_{2,j} V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{2,j} V'_{2,j}}] \cdot \psi'_{2,j} = [\frac{a_{1,j} V'_{1,j}}{\psi'_{2,j} V'_{2,j}}] \cdot \psi'_{2,j}.$$

Основами в отриманий вираз співвідношення для вагових коефіцієнтів $V'_{1,j}$ і $V'_{2,j}$:

$$V'_{2,j} = \prod_{i=3}^{m+1} \psi_{i,j}; V'_{1,j} = \psi'_{2,j} \cdot \prod_{i=3}^{m+1} \psi_{i,j}.$$

Тоді отримаємо:

$$[\frac{a_{1,j} V'_{1,j}}{\psi'_{2,j} V'_{2,j}}] \cdot \psi'_{2,j} = [\frac{a_{1,j} \cdot \psi'_{2,j} \cdot \prod_{i=3}^{m+1} \psi_{i,j} \cdot \psi'_{2,j}}{\psi'_{2,j} \cdot \prod_{i=3}^{m+1} \psi_{i,j}}] = a_{1,j} \cdot \psi'_{2,j}.$$

Запишемо вираз (4.16) з урахуванням перетвореної лівої і правої частини. В цьому випадку отримаємо:

$$a''_{2,j} = a_{1,j} \cdot \psi'_{2,j} + a'_{2,j} - a_{1,j} \cdot \psi'_{2,j} = a'_{2,j}.$$

Значить, значення $a''_{2,j}$ вбудованого елемента, що реконструюється авторизованим користувачем на приймальній стороні збігається з вихідним значенням $a'_{2.j}$ приховуваного повідомлення на передавальній стороні.

3. Мінімізацію спотворень вихідного зображення. Такі спотворення залежать від значення $\Delta N(j)$ пульсації стеганокода. Процес вбудовування інформації збільшує значення коду-контейнера на величину $\Delta N(j)$. Значення пульсації стеганокода визначається за формулою:

$$\Delta N(j) = \left(\sum_{i=1}^{\gamma-1} a_{i,j} V'_{i,j} (\psi'_{\gamma,j} - 1)\right) + a'_{\gamma,j} V'_{\gamma,j} =$$

$$= a_{1,j} V'_{1,j} + V'_{2,j}.$$

Звідси, вбудовування елемента $a'_{2,j} = 1$ на позицію $\gamma = 2$ другого елемента знижує кількість $\Delta N(j)$ спотворень внесених встраиванием в стеганокод $N(j)'$ щодо значення коду-контейнера $N(j)$. Однак, при цьому зберігається стійкість вбудованих даних, так як значення вагового коефіцієнта $V'_{2,j}$ приймає максимально значення для $\gamma = \overline{2,\ m+1}$ позицій вбудовування, тобто:

$$V'_{2,j} = \max_{2 \le i \le m+1} \{V'_{i,j}\}.$$

Розглянемо функціонування стеганографічної системи на основі корекції нерівновагового базису основ рис. 4.1. Імплантація виконується у виявленні сегменти з низьким та середнім рівнем насиченності структурними деталями з метою зменшення рівня ПВСШ при декодуванні неавторизованним користувачем. Дана система дозволяє вбудувати біт приховуваного повідомлення на другу позицію нерівновагового позиційного числа в процесі стеганографічного кодування. Отримана в результаті такого кодування стеганограмма складається з інформаційної та модифікованої службової частин.

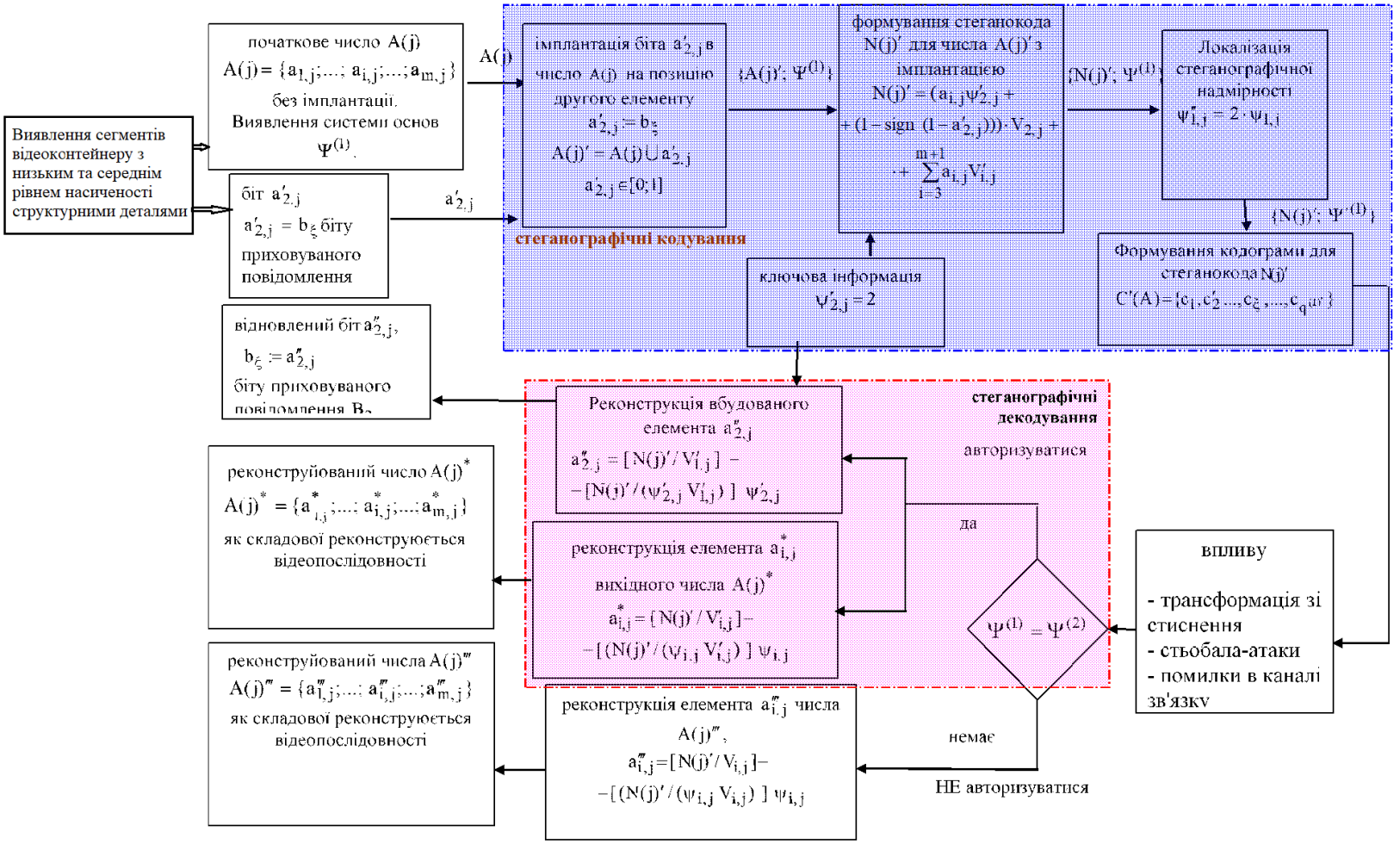

Рисунок 4.1 - Структурна схема стеганографічної системи на основі імплантації приховуваного двійкового елемента на другу позицію НПЧ з подальшим кодуванням і маскування базису основ

Реалізація вилучення вбудованих даних відбувається по біполярному принципом: для авторизованого та неавторизованого користувача [4].

Стеганографічна система включає в себе наступні этапи:

I. Стеганографічне кодування з корекцією нерівновагового базису основ $\Psi'^{(1)}$.

Розглянемо процес стеганографічного кодування. Даний етап включає в себе наступні дії:

1. Імплантацію елемента b_ξ на позицію другого елементу числа $A(j)$. Тут b_ξ-ξ-й елемент вбудовується послідовності $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0; 1]$, $\xi = \overline{1, \nu}$. Імплантація задається наступною формулою

$$A(j)' = A(j) \cup b_\xi; b_\xi = a'_{2,j} \in [0,\ 1]. \tag{4.19}$$

В результаті імплантації, число $A(j)'$ прийме наступний вигляд:

$$A(j)' = \{ a_{1,j}; a'_{2,j};...; a_{i,j};...; a_{m+1,j} \}, \tag{4.20}$$

де $A(j)'$ - число з імплантованим на другу позицію елементом $a'_{2,j}$.

2. Формування стеганокода $N(j)'$ для числа $A(j)'$ з імплантованим елементом $a'_{2,j}$ за формулою

$$N'(j) = a_{1,j} V'_{1,j} + a'_{2,j} V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j} V'_{i,j}; \tag{4.21}$$

$$V'_{2,j} = \prod_{i=3}^{m+1} \psi_{i,j};$$

$$V'_{1,j} = \psi'_{2,j} \cdot \prod_{i=3}^{m+1} \psi_{i,j}, \qquad (4.22)$$

де $V'_{i,j}$ - ваговий коефіцієнт елемента $a_{i,j}$ НПЧ з імплантацією;

$V'_{1,j}$-ваговий коефіцієнт першого елемента НПЧ з імплантацією;

$V'_{2,j}$ - ваговий коефіцієнт імплантованого елемента, що дорівнює добутку всіх наступних основ;

$\psi'_{2,j}$- основа імплантованого елемента;

$\psi_{i,j}$ - основа $(i;\ j)$-го елемента числа $A(j)'$ з імплантацією.

ваговий коефіцієнт $V'_{i,j}$ елемента $a_{i,j}$, Позиція якого в числі $A(j)'$ молодше позиції імплантованого елемента $a'_{2,j}$, Тобто $i = \overline{3, m+1}$, Обчислюється за формулою:

$$V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}. \qquad (4.24)$$

З врахуванням того, що $a'_{2,j} \in [0;1]$, Перетворимо отриманий вираз до наступного вигляду:

$$N'(j) = \begin{cases} a_{1,j} V'_{1,j} + \sum_{i=3}^{m+1} a_{i,j} V'_{i,j}, & \to a'_{2,j} = 0; \\ a_{1,j} V'_{1,j} + V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j} V'_{i,j} = & \\ = (a_{1,j}\psi'_{2,j} + 1) \cdot V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j} V'_{i,j}, & \to a'_{2,j} = 1. \end{cases}$$

або використовуючи функцію sign, отримаємо:

$$N(j)' = a_{1,j}V'_{1,j} + (1 - \text{sign}\ (1 - a'_{2,j})) \cdot V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}$$

або

$$N(j)' = (a_{1,j}\psi'_{2,j} + (1 - \text{sign}\ (1 - a'_{2,j}))) \cdot V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}.$$

3. Локалізація структурної стеганографічної надмірності шляхом корекції нерівновагового позиційного базису $\Psi^{(1)}$. Дана операція проводиться для усунення можливості для зловмисника встановити факт наявності вбудовування інформації. Корекція нерівновагового базису здійснюється шляхом збільшення в два рази основи першого елемента $\psi_{1,j}$, Тобто:

$$\psi''_{1,j} = \psi_{1,j} \cdot 2.$$

У разі застосування такої корекції модифікована система основі $\Psi'^{(1)}$ після вбудовування прийме наступний вигляд:

$$\Psi'^{(1)} = \{2 \cdot \psi_{1,j}; \psi_{2,j}; ...; \psi_{i,j}; ...; \psi_{m,j}\} = \{\psi''_{1,j}; \psi_{2,j}; ...; \psi_{i,j}; ...; \psi_{m,j}\}.$$

Скоригований базис основ $\Psi'^{(1)}$ буде застосовуватися при декодуванні неавторизованих користувачів.

4. Формування кодограми C'_j для кодового представлення стеганокода $N(j)'$:

$$C'_j = \{c_1, ..., c_\tau, ..., c_{q(j)'}\},$$

де $q(j)'$ - довжина кодограми C'_j, що дорівнює $q(j)' = [(\sum_{i=1}^{m+1} \ell og_2 \psi_{i,j})] + 1$.

На рисунку 4.2 схематично відображені етапи стеганографічного кодування в умовах імплантації біта на позицію другого елементу нерівновагового позиційного числа.

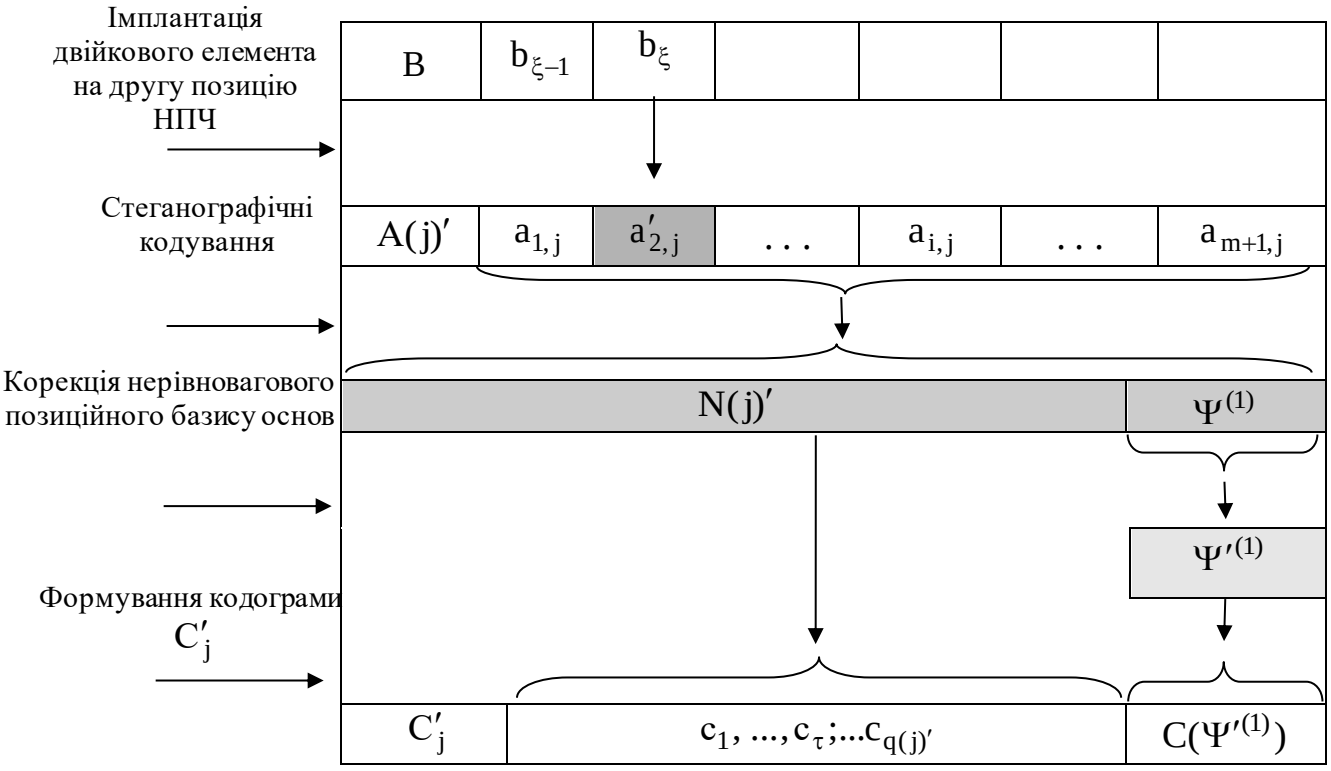

Рисунок 4.2 - Структурна схема побудови кодограми стеганокода для числа $A'(j)$ з імплантацією на другій позиції

II. Розглянемо процес стеганографічного декодування даних, що містяться в стеганограмме. Процес стеганографічного декодування в даному випадку здійснюється по біполярному принципом для авторизованого користувача і зловмисника (неавторизований користувач).

У разі неавторизованого доступу у зловмисника відсутня інформація:

- про позицію вбудовування елемента $a'_{2,j}$;

- про позицію стеганокода в стислому представленні зображення.

Тоді процес декодування здійснюється на основі наступних етапів (рис 4.3):

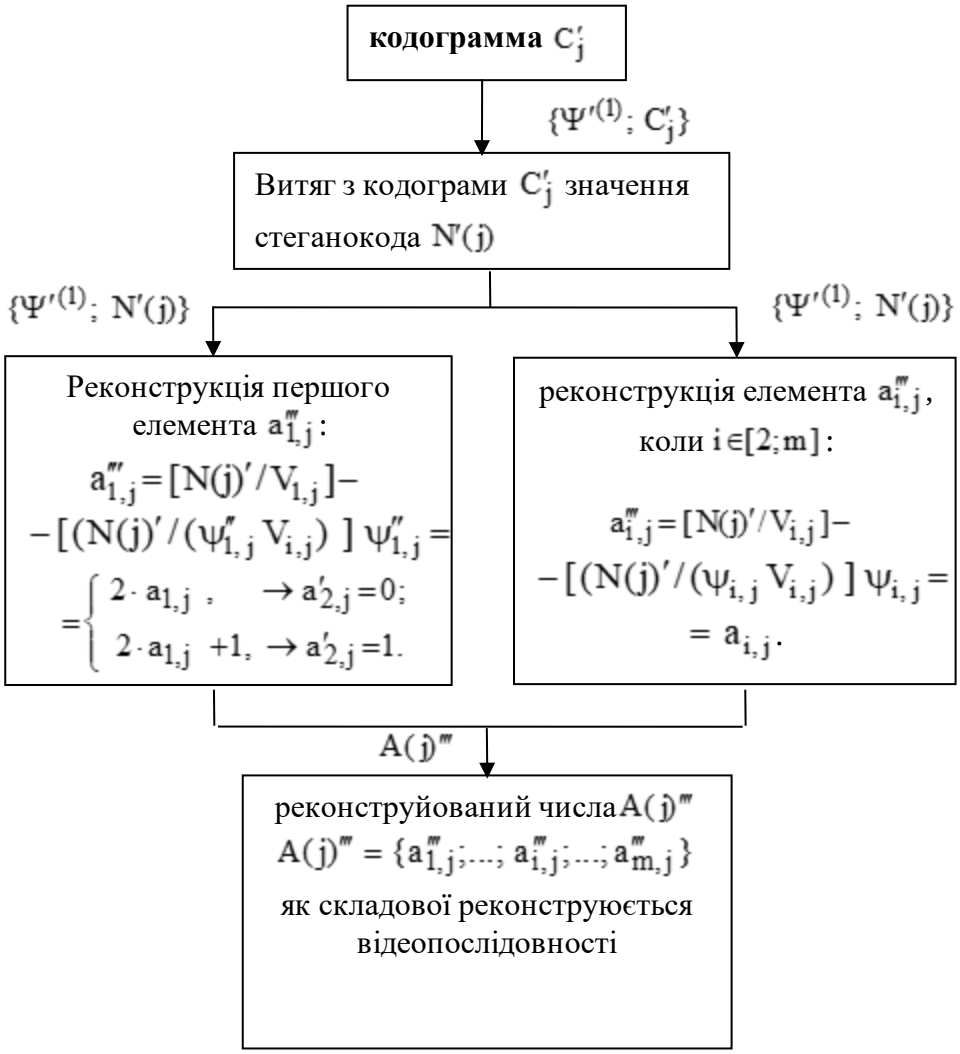

Рисунок 4.3 - Схема декодування стеганокода при неавторизований доступ

1. Витяг з кодограми C'_j стеганокода $N(j)'$ за допомогою модифікованої системи основ $\Psi'^{(1)}$.

2. Відновлення елементів вихідної відеопослідовності.

Тут реконструкція елементів $a'''_{i,j}$ буде здійснюватися на основі модифікованої системи основ $\Psi'^{(1)}$. Звідси відновленні першого елемента $a'''_{1,j}$ вихідної відеопослідовності буде здійснюватися на основі скоригованого основи $\psi''_{1,j}$ за формулою:

$$a'''_{1,j} = [\,N(j)'/V_{1,j}\,] - [\,N(j)'/(\psi''_{1,j}\,V_{1,j})\,]\,\psi''_{1,j}. \qquad (4.24)$$

Розпишемо цей вислів з урахуванням формули для стеганокода:

$$N(j)' = a_{1,j}V'_{1,j} + a'_{2,j}V'_{1,j} + \sum_{i=3}^{m+1} a_{i,j}\overline{V}_{i,j}.$$

В цьому випадку отримаємо:

$$a'''_{1,j} = [(a_{1,j}V'_{1,j} + a'_{2,j}V'_{1,j} + \sum_{i=3}^{m+1} a_{i,j}\overline{V}_{i,j})/V_{1,j}] -$$

$$-[(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}\overline{V}_{i,j})/(\psi''_{1,j}V_{1,j})]\cdot\psi''_{1,j}.$$

Перепишемо цей вислів з огляду на таке співвідношення:

$$\overline{V}_{i,j} = V_{i-1,j}.$$

Тоді отримаємо:

$$a'''_{1,j} = [(a_{1,j}V'_{1,j} + a'_{2,j}V'_{1,j} + \sum_{i=2}^{m} a_{i,j}V_{i,j})/V_{1,j}] -$$

$$-[(a_{1,j}V'_{1,j}+a'_{2,j}V'_{2,j}+\sum_{i=2}^{m}a_{i,j}V_{i,j})/(\psi''_{1,j}V_{1,j})]\cdot\psi''_{1,j}=$$

$$=[\frac{a_{1,j}V'_{1,j}}{V_{1,j}}+\frac{a'_{2,j}V'_{2,j}}{V_{1,j}}+\frac{\sum_{i=2}^{m}a_{i,j}V_{i,j}}{V_{1,j}}]-$$

$$-[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V_{1,j}}+\frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V_{1,j}}+\frac{\sum_{i=2}^{m}a_{i,j}V_{i,j}}{\psi''_{1,j}V_{1,j}}]\cdot\psi''_{1,j}. \quad (4.25)$$

Перетворимо перший доданок правої частини виразу (4.25):

$$[\frac{a_{1,j}V'_{1,j}}{V_{1,j}}+\frac{a'_{2,j}V'_{2,j}}{V_{1,j}}+\frac{\sum_{i=2}^{m}a_{i,j}V_{i,j}}{V_{1,j}}]. \quad (4.26)$$

Третє складова даного вираження з урахуванням нерівності

$$\sum_{i=3}^{m+1}a_{i,j}\overline{V}_{i,j}=\sum_{i=2}^{m}a_{i,j}V_{i,j}<V_{1,j}$$

прийме значення менше одиниці, тобто:

$$\sum_{i=3}^{m+1}a_{i,j}V'_{i,j}<1.$$

Перетворимо перший доданок виразу (4.26) з урахуванням наступного співвідношення для вагового коефіцієнта $V'_{1,j}$:

$$V'_{1,j}=\psi'_{\gamma,j}V_{1,j}. \quad (4.27)$$

Тоді отримаємо:

$$\left[\frac{a_{1,j}V'_{1,j}}{V_{1,j}}\right] = \left[\frac{a_{1,j}\,\psi'_{\gamma,j}\cdot V_{1,j}}{V_{1,j}}\right] = a_{1,j}\,\psi'_{\gamma,j}.$$

Розпишемо другий доданок виразу (4.26) з урахуванням нерівності:

$$V'_{2,j} = V_{1,j}. \tag{4.28}$$

У цьому випадку воно прийме наступний вигляд:

$$\left[\frac{a'_{2,j}V'_{2,j}}{V_{1,j}}\right] = \left[\frac{a'_{2,j}V_{1,j}}{V_{1,j}}\right] = a'_{2,j}.$$

Перепишемо вираз (4.11) з урахуванням перетворених доданків:

$$\left[\frac{a_{1,j}V'_{1,j}}{V_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{V_{1,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{V_{1,j}}\right] = a_{1,j}\,\psi'_{\gamma,j} + a_{1,j}. \tag{4.29}$$

Тепер розглянемо другий доданок правої частини виразу (4.25):

$$\left[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V_{1,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{\psi''_{1,j}V_{1,j}}\right]\cdot\psi''_{1,j}. \tag{4.30}$$

Перепишемо перший доданок вираження (4.30) з урахуванням нерівності (4.27). У цьому випадку воно прийме наступний вигляд:

$$\left[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V_{1,j}}\right] = \left[\frac{a_{1,j}\cdot\psi'_{\gamma,j}V_{1,j}}{\psi''_{1,j}V_{1,j}}\right] = \left[\frac{a_{1,j}\cdot\psi'_{\gamma,j}}{\psi''_{1,j}}\right].$$

Перетворимо дане вираження з урахуванням наступних співвідношень:

$$\psi''_{1,j} = 2\psi_{1,j},\ \psi_{\gamma,j} = 2.$$

Тоді перший доданок прийме значення менше одиниці, тобто:

$$\left[\frac{a_{1,j}\cdot\psi'_{\gamma,j}}{\psi''_{1,j}}\right] = \left[\frac{2\cdot a_{1,j}}{2\cdot\psi_{1,j}}\right] = \left[\frac{a_{1,j}}{\psi_{1,j}}\right] < 1$$

або

$$\left[\frac{a_{1,j}\cdot\psi'_{\gamma,j}}{\psi''_{1,j}}\right] = \left[\frac{2\cdot a_{1,j}}{2\cdot\psi_{1,j}}\right] = \left[\frac{a_{1,j}}{\psi_{1,j}}\right] = 0.$$

Розглянемо другий доданок правої частини виразу (4.30) з урахуванням наступних співвідношень:

$$\psi''_{1,j} = 2\psi_{1,j},\ V'_{2,j} = V_{1,j}.$$

В цьому випадку отримаємо:

$$\left[\frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V_{1,j}}\right] = \left[\frac{a'_{2,j}V_{1,j}}{2\cdot\psi_{1,j}V_{1,j}}\right] = \left[\frac{a'_{2,j}}{2\cdot\psi_{1,j}}\right].$$

Третє складова виразу (4.30) з урахуванням співвідношення

$$\psi''_{1,j} V_{1,j} > \frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{\psi''_{1,j} V_{1,j}}$$

прийме значення менше одиниці, тобто:

$$[\frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{\psi''_{1,j} V_{1,j}}] < 1.$$

отже

$$[\frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{\psi''_{1,j} V_{1,j}}] = 0.$$

Тепер перепишемо значення другого доданка правої частини виразу (4.25) з урахуванням виконаних перетворень:

$$[\frac{a_{1,j} V'_{1,j}}{\psi''_{1,j} V_{1,j}} + \frac{a'_{2,j} V'_{2,j}}{\psi''_{1,j} V_{1,j}} + \frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{\psi''_{1,j} V_{1,j}}] \cdot \psi''_{1,j} = [\frac{a'_{2,j}}{2 \cdot \psi_{1,j}}] \cdot \psi''_{1,j} = 0.$$

Тоді значення елемента $a'''_{1,j}$ буде визначатися на основі наступного співвідношення:

$$a'''_{1,j} = a_{1,j}\ \psi'_{\gamma,j} + a_{1,j} = \begin{cases} 2 \cdot a_{1,j}\ , & \to a'_{2,j} = 0; \\ 2 \cdot a_{1,j}\ + 1, & \to a'_{2,j} = 1. \end{cases}$$

Реконструкція інших елементів $a'''_{i,j}$, коли i приймає значення $i = \overline{2, m}$ описується виразом:

$$a'''_{i,j} = [N(j)'/V_{i,j}] - [N(j)'/(\psi_{i,j} V_{i,j})]\ \psi_{i,j}, \qquad (4.31)$$

де $a'''_{i,j}$- i-й елемент реконструюється числа $A(j)'''$, як складової реконструюється j-й відеопослідовності при неавторизований доступ.

Розпишемо цей вираз з урахуванням співвідношення для стеганокода:

$$N(j)' = a_{1,j} V'_{1,j} + a'_{2,j} V'_{1,j} + \sum_{i=3}^{m+1} a_{i,j} \overline{V}_{i,j}.$$

Тоді отримаємо:

$$a'''_{i,j} = [(a_{1,j} V'_{1,j} + a'_{2,j} V'_{1,j} + \sum_{i=3}^{m+1} a_{i,j} \overline{V}_{i,j}) / V_{i,j}] -$$

$$-[(a_{1,j} V'_{1,j} + a'_{2,j} V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j} \overline{V}_{i,j}) / (\psi_{i,j} V_{i,j})] \cdot \psi_{i,j}.$$

Перепишемо цей вислів з огляду на таке співвідношення:

$$\overline{V}_{i,j} = V_{i-1,j}.$$

В цьому випадку отримаємо:

$$a'''_{i,j} = [(a_{1,j} V'_{1,j} + a'_{2,j} V'_{1,j} + \sum_{i=2}^{m} a_{i,j} V_{i,j}) / V_{i,j}] -$$

$$-[(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=2}^{m} a_{i,j}V_{i,j}) / (\psi_{i,j}V_{i,j})] \cdot \psi_{1,j} =$$

$$= [\frac{a_{1,j}V'_{1,j}}{V_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{V_{i,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{V_{i,j}}] -$$

$$-[\frac{a_{1,j}V'_{1,j}}{\psi_{i,j}V_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi_{i,j}V_{i,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{\psi_{i,j}V_{i,j}}] \cdot \psi_{i,j} . \quad (4.32)$$

Розглянемо перший доданок правої частини виразу (4.32):

$$[\frac{a_{1,j}V'_{1,j}}{V_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{V_{i,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{V_{i,j}}] . \quad (4.33)$$

Перепишемо перший доданок виразу (4.33) з огляду на таке співвідношення для вагового коефіцієнта $V'_{1,j}$:

$$V'_{1,j} = \psi'_{\gamma,j} V_{1,j} .$$

В цьому випадку отримаємо:

$$[\frac{a_{1,j}V'_{1,j}}{V_{i,j}}] = [a_{1,j}\psi'_{\gamma,j}\frac{V_{1,j}}{V_{i,j}}].$$

Тепер перетворимо отриманий вираз з урахуванням формул для вагових коефіцієнтів $V_{1,j}$ і $V_{i,j}$:

$$V_{1,j} = \prod_{\xi=2}^{m} \psi_{\xi,j}, \tag{4.34}$$

$$V_{i,j} = \prod_{\xi=i+1}^{m} \psi_{\xi,j}. \tag{4.35}$$

Тоді перший доданок виразу (4.33) набуде вигляду:

$$[\frac{a_{1,j} V'_{1,j}}{V_{i,j}}] = [a_{1,j} \psi'_{\gamma,j} \frac{V_{1,j}}{V_{i,j}}] = [a_{1,j} \psi'_{\gamma,j} \frac{\prod_{\xi=2}^{m} \psi_{\xi,j}}{\prod_{\xi=i+1}^{m} \psi_{\xi,j}}] = a_{1,j} \psi'_{\gamma,j} \prod_{\xi=2}^{i} \psi_{\xi,j}.$$

Тепер перепишемо другий доданок вираження (4.33) з урахуванням наступного співвідношення:

$$V'_{2,j} = V_{1,j}.$$

Тоді отримаємо:

$$[\frac{a'_{2,j} V'_{2,j}}{V_{i,j}}] = [\frac{a'_{2,j} V_{1,j}}{V_{i,j}}].$$

Тепер перетворимо другий доданок вираження (4.33) з урахуванням формул (4.33) і (4.35). В цьому випадку отримаємо:

$$[\frac{a'_{2,j} V'_{2,j}}{V_{i,j}}] = [\frac{a'_{2,j} V_{1,j}}{V_{i,j}}] = [\frac{\prod_{\xi=2}^{m} \psi_{\xi,j}}{\prod_{\xi=i+1}^{m} \psi_{\xi,j}}] = a'_{2,j} \prod_{\xi=2}^{i} \psi_{\xi,j}.$$

Розглянемо третій доданок виразу (4.33):

$$[\frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{V_{i,j}}] = [\frac{\sum_{\xi=2}^{i} a_{\xi,j} V_{\xi,j} + \sum_{\xi=i+1}^{m} a_{\xi,j} V_{\xi,j}}{V_{i,j}}].$$

Перепишемо цей вислів, з огляду на наступне співвідношення:

$$V_{i,j} > \sum_{\xi=i+1}^{m} a_{\xi,j} V_{\xi,j}.$$

Тоді отримаємо:

$$[\frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{V_{i,j}}] = [\frac{\sum_{\xi=2}^{i} a_{\xi,j} V_{\xi,j}}{V_{i,j}}].$$

Перепишемо отримане вираз з урахуванням формули (4.35):

$$[\frac{\sum_{\xi=2}^{i} a_{\xi,j} V_{\xi,j}}{V_{i,j}}] = [\frac{\sum_{\xi=2}^{i} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{m} \psi_{\alpha,j}}{\prod_{\xi=i+1}^{m} \psi_{\xi.j}}] = \sum_{\xi=2}^{i} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j}.$$

Перепишемо вираз (4.34) З урахуванням виконаних перетворень. В цьому випадку отримаємо:

$$[\frac{a_{1,j}V'_{1,j}}{V_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{V_{i,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{V_{i,j}}] =$$

$$= [a_{1,j}\psi'_{\gamma,j}\prod_{\xi=2}^{i}\psi_{\xi} + a'_{2,j}\prod_{\xi=2}^{i}\psi_{\xi} + \sum_{\xi=2}^{i}a_{\xi,j}\cdot\prod_{\alpha=\xi+1}^{i}\psi_{\xi,j}].$$

Тепер розглянемо другий доданок правої частини виразу (4.32):

$$[\frac{a_{1,j}V'_{1,j}}{\psi_{i,j}V_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi_{i,j}V_{i,j}} + \frac{\sum_{i=2}^{m} a_{i,j}V_{i,j}}{\psi_{i,j}V_{i,j}}]\cdot\psi_{i,j}. \qquad (4.36)$$

Перепишемо перший доданок виразу (4.36) з огляду на таке співвідношення:

$$V'_{1,j} = \psi'_{\gamma,j}V_{1,j}.$$

В цьому випадку отримаємо:

$$[\frac{a_{1,j}V'_{1,j}}{\psi_{i,j}V_{i,j}}] = [\frac{a_{1,j}\psi'_{\gamma,j}V_{1,j}}{\psi_{i,j}V_{i,j}}].$$

Перепишемо отримане вираз з урахуванням формул (4.34) і (4.35). Тоді отримаємо:

$$[\frac{a_{1,j}V'_{1,j}}{\psi_{i,j}V_{i,j}}] = [\frac{a_{1,j}\psi'_{\gamma,j}\prod_{\xi=2}^{m}\psi_{\xi,j}}{\psi_{i,j}\prod_{\xi=i+1}^{m}\psi_{\xi,j}}] = [\frac{a_{1,j}\psi'_{\gamma,j}\prod_{\xi=2}^{i}\psi_{\xi,j}}{\psi_{i,j}}] = a_{1,j}\psi'_{\gamma,j}\prod_{\xi=2}^{i-1}\psi_{\xi,j}.$$

Тепер розглянемо другий доданок виразу (4.36) з урахуванням формул (4.34) і (4.35):

$$[\frac{a'_{2,j}V'_{2,j}}{\psi_{i,j}V_{i,j}}] = [\frac{a'_{2,j}V_{1,j}}{\psi_{i,j}V_{i,j}}] = [a'_{2,j}\frac{\prod_{\xi=2}^{m}\psi_{\xi,j}}{\psi_{i,j}\prod_{\xi=i+1}^{m}\psi_{\xi,j}}] =$$

$$= [a'_{2,j}\frac{\prod_{\xi=2}^{m}\psi_{\xi,j}}{\prod_{\xi=i}^{m}\psi_{\xi,j}}] = a'_{2,j}\prod_{\xi=2}^{i-1}\psi_{\xi,j}\,.$$

Розглянемо третій доданок вираження (4.36) з урахуванням наступного співвідношення:

$$\psi_{i,j}V_{i,j} > \sum_{\xi=i}^{m}a_{i,j}V_{i,j}.$$

В цьому випадку отримаємо:

$$[\frac{\sum_{i=2}^{m}a_{i,j}V_{i,j}}{\psi_{i,j}V_{i,j}}] = [\frac{\sum_{\xi=2}^{i-1}a_{\xi,j}V_{\xi,j} + \sum_{\xi=i}^{m}a_{\xi,j}V_{\xi,j}}{\psi_{i,j}V_{i,j}}] = [\frac{\sum_{\xi=2}^{i-1}a_{\xi,j}V_{\xi,j}}{\psi_{i,j}V_{i,j}}].$$

Перепишемо отримане вираз з урахуванням формули (4.35). Тоді отримаємо:

$$\left[\frac{\sum_{\xi=2}^{i-1} a_{\xi,j} V_{\xi,j}}{\psi_{i,j} V_{i,j}}\right] = \left[\frac{\sum_{\xi=2}^{i-1} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{m} \psi_{\alpha,j}}{\psi_{i,j} \prod_{\xi=i+1}^{m} \psi_{\xi.j}}\right] = \sum_{\xi=2}^{i-1} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i-1} \psi_{\alpha,j} \cdot$$

Тепер перепишемо другий доданок правої частини виразу (4.32) з урахуванням виконаних перетворень:

$$\left[\frac{a_{1,j} V'_{1,j}}{\psi_{i,j} V_{i,j}} + \frac{a'_{2,j} V'_{2,j}}{\psi_{i,j} V_{i,j}} + \frac{\sum_{i=2}^{m} a_{i,j} V_{i,j}}{\psi_{i,j} V_{i,j}}\right] \cdot \psi_{i,j} =$$

$$\left[a_{1,j} \psi'_{\gamma,j} \prod_{\xi=2}^{i-1} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=2}^{i-1} \psi_{\xi,j} + \sum_{\xi=2}^{i-1} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i-1} \psi_{\alpha,j}\right] \psi_{i,j} =$$

$$= a_{1,j} \psi'_{\gamma,j} \prod_{\xi=2}^{i} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=2}^{i} \psi_{\xi,j} + \sum_{\xi=2}^{i-1} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} \cdot$$

Перепишемо вираз (4.32) з урахуванням перетвореної правій частині. В цьому випадку вираз (4.32) прийме наступний вигляд:

$$a'''_{i,j} = a_{1,j} \psi'_{\gamma,j} \prod_{\xi=2}^{i} \psi_{\xi} + a'_{2,j} \prod_{\xi=2}^{i} \psi_{\xi} + \sum_{\xi=2}^{i} a_{\xi,j} V_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i} \psi_{\xi,j} -$$

$$- a_{1,j} \psi'_{\gamma,j} \prod_{\xi=2}^{i} \psi_{\xi,j} - a'_{2,j} \prod_{\xi=2}^{i} \psi_{\xi,j} - \sum_{\xi=2}^{i-1} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} =$$

$$= \sum_{\xi=2}^{i} a_{\xi,j} V_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} - \sum_{\xi=2}^{i-1} a_{\xi,j} \cdot \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} = a_{i,j}$$

Звідси, в разі неавторизованого доступу відновлення першого елемента $a'''_{1,j}$ числа $A'''(j)$ вихідної відеопослідовності здійснюється з внесенням

похибки. Відновлення інших елементів $a'''_{i,j}$, коли $i \in [2; m]$, здійснюється без помилок.

3. Оцінка якості візуального сприйняття реконструюється зображення, тобто проведення атаки щодо факту наявності вбудованої інформації.

Тепер розглянемо процес стеганографічного декодування при авторизованому доступі (рис. 4.4):

В цьому випадку користувачеві доступна наступна інформація:

а) позиція стеганокода в стислому представленні зображення;

б) позиція вбудованого елемента $a'_{2,j}$;

в) основа $\psi'_{2,j}$ вбудованого елемента. $a'_{2,j}$.

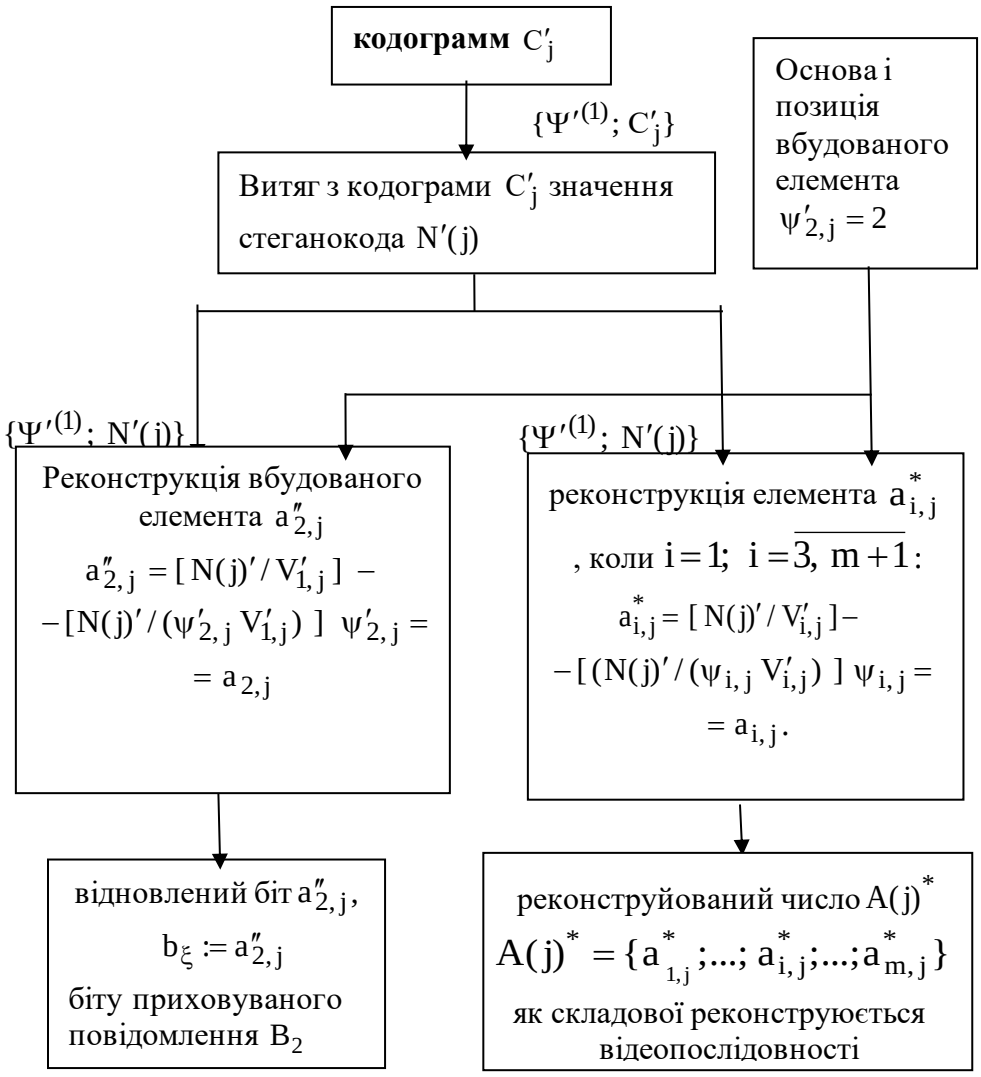

Рисунок 4.4 - Схема декодування стеганокода при авторизованому доступі

В цьому випадку стеганографічне декодування буде містити наступні етапи:

1. Витяг з кодограми C'_j значення стеганокода $N(j)'$.

2. Відновлення вбудованого елемента $a'_{2,j}$. Даний етап реалізується на основі інформації про позицію вбудованого елемента і його заснування $\psi'_{2,j} = 2$. Для цього використовується формула (4.16):

$$a''_{2,j} = [\, N(j)' / V'_{2,j} \,] - [\, N(j)' / (\psi'_{2,j} V'_{1,j}) \,] \; \psi'_{2,j}.$$

тут $a''_{2,j}$ - значення вилученого біта вбудованої інформації, $b_\xi := a''_{2,j}$.

3. Відновлення інших елементів $a^*_{i,j}$ вихідної відеопослідовності буде проводитися на основі модифікованої системи основ $\Psi'^{(1)}$. В даному випадку можливо демаскування структурної стеганографічної надмірності шляхом відновлення початкового значення $\psi_{1,j}$ на основі виразу:

$$\psi_{1,j} = \psi''_{1,j} / 2.$$

Беручи до уваги те, що значення модифікованого основи $\psi''_{1,j}$ не враховується при реконструкції елементів $a^*_{i,j}$, стеганографічне декодуванням будемо проводити без демаскування структурної стеганографічної надмірності. Це дозволити скоротити кількість операцій при стеганографічному декодуванні. Тоді значення першого елемента $a^*_{1,j}$ буде обчислюватися за формулою:

$$a^*_{1,j} = [\, N(j)' / V'_{1,j} \,] - [\, N(j)' / (\psi''_{1,j} V'_{i,j}) \,] \; \psi''_{1,j}. \qquad (4.37)$$

Розпишемо цей вираз з урахуванням формули:

$$N(j)' = a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j},$$

Тоді отримаємо:

$$a^{*}_{1,j} = [(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}) / V'_{1,j}] -$$

$$-[(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}) / (\psi''_{1,j}V'_{1,j})] \cdot \psi''_{1,j} =$$

$$= [\frac{a_{1,j}V'_{1,j}}{V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{1,j}}] -$$

$$-[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi''_{1,j}V'_{1,j}}] \cdot \psi''_{1,j}. \quad ()$$

Розглянемо перший доданок правої частини виразу (4.38):

$$[\frac{a_{1,j}V'_{1,j}}{V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{1,j}}]. \quad (4.39)$$

Перетворимо вираження (4.39) з урахуванням наступного нерівності:

$$V'_{1,j} > \sum_{i=2}^{m+1} a_{i,j}V'_{i,j}.$$

В цьому випадку друге і третє складові виразу (4.39) прийматимуть значення менше одиниці, тобто:

$$\frac{a'_{2,j}V'_{2,j}}{V'_{1,j}} < 1; \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{1,j}} < 1.$$

Тоді перший доданок правої частини виразу (4.38) прийме наступний вигляд:

$$[\frac{a_{1,j}V'_{1,j}}{V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{1,j}}] = [\frac{a_{1,j}V'_{1,j}}{V'_{1,j}}] = a_{1,j}.$$

Тепер розглянемо другий доданок правої частини виразу (4.38):

$$[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi''_{1,j}V'_{1,j}}] \cdot \psi''_{1,j} \quad (4.40)$$

перетворимо вираз (4.40) з урахуванням наступного нерівності:

$$\psi''_{1,j}V'_{1,j} > a'_{2,j}V'_{2,j}.$$

В цьому випадку друге і третє складові виразу (4.40) прийматимуть значення менше одиниці, тобто:

$$\frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V'_{1,j}} < 1, \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi''_{1,j}V'_{2,j}} < 1.$$

Перший доданок прийме наступний вигляд:

$$[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{1,j}}] = [\frac{a_{1,j}}{\psi''_{1,j}}].$$

Перепишемо отримане вираз з урахуванням наступного співвідношення:

$$\psi''_{1,j} > a_{1,j}.$$

У цьому випадку перший доданок вираження (4.40) прийме значення менше одиниці:

$$[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{1,j}}] = [\frac{a_{1,j}}{\psi''_{1,j}}] < 1$$

або

$$[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{1,j}}] = [\frac{a_{1,j}}{\psi''_{1,j}}] = 0.$$

Звідси другий доданок правої частини виразу (4.38) прийме значення менше одного:

$$[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi''_{1,j}V'_{1,j}}] \cdot \psi''_{1,j} < 1.$$

отже

$$[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi''_{1,j}V'_{1,j}}]\cdot\psi''_{1,j} = 0.$$

Перепишемо вираз (4.38) з урахуванням виконаних перетворень:

$$a^*_{1,j} = [\frac{a_{1,j}V'_{1,j}}{V'_{1,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{1,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{1,j}}] -$$

$$-[\frac{a_{1,j}V'_{1,j}}{\psi''_{1,j}V'_{2,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi''_{1,j}V'_{2,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi''_{1,j}V'_{1,j}}]\cdot\psi''_{1,j} = a_{1,j}$$

Значення інших елементів $i = \overline{3, m+1}$ вихідної відеопослідовності декодируется на основі наступного виразу:

$$a^*_{i,j} = [N(j)'/V'_{i,j}] - [N(j)'/(\psi_{i,j}V'_{i,j})]\psi_{i,j}, \qquad (4.41)$$

Де $a^*_{i,j}$ - i-й елемент числа $A(j)^*$, як складової реконструюється вихідної j-й відеопослідовності при авторизованому доступі.

Розпишемо цей вислів з огляду на таке співвідношення для стеганокода $N(j)'$:

$$N(j)' = a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}.$$

Тоді отримаємо:

$$a^{*}_{i.j} = [(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}) / V'_{i,j}] -$$

$$-[(a_{1,j}V'_{1,j} + a'_{2,j}V'_{2,j} + \sum_{i=3}^{m+1} a_{i,j}V'_{i,j}) / (\psi_{i,j}V'_{i,j})] \cdot \psi_{i,j} =$$

$$= [\frac{a_{1,j}V'_{1,j}}{V'_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{i,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{i,j}}] -$$

$$-[\frac{a_{1,j}V'_{1,j}}{\psi_{i,j}V'_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi_{i,j}V'_{i,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{\psi_{i,j}V'_{i,j}}] \cdot \psi_{i,j} . \qquad (4.42)$$

Розглянемо перший доданок правої частини виразу (4.42):

$$[\frac{a_{1,j}V'_{1,j}}{V'_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{V'_{i,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{i,j}}] . \qquad (4.43)$$

Перетворимо третій доданок виразу (4.43) з урахуванням наступного нерівності:

$$V'_{i,j} > \sum_{\xi=i+1}^{m+1} a_{i,j}V_{i,j} . \qquad (4.44)$$

В цьому випадку отримаємо:

$$[\frac{\sum_{i=3}^{m+1} a_{i,j}V'_{i,j}}{V'_{i,j}}] = [\frac{\sum_{\xi=3}^{i} a_{\xi,j}V_{\xi,j} + \sum_{\xi=i+1}^{m+1} a_{\xi,j}V'_{\xi,j}}{V'_{i,j}}] = [\frac{\sum_{\xi=3}^{i} a_{\xi,j}V'_{\xi,j}}{V'_{i,j}}].$$

Перепишемо отримане вираз з урахуванням наступного співвідношення для вагового коефіцієнта $V'_{i,j}$:

$$V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j} .$$

Тоді отримаємо:

$$\left[\frac{\sum_{\xi=3}^{i+1} a_{\xi,j} V'_{\xi,j}}{V'_{i,j}}\right] = \left[\frac{\sum_{\xi=3}^{i+1} a_{\xi,j} \prod_{\alpha=\xi+1}^{m+1} \psi_{\alpha,j}}{\prod_{\xi=i+1}^{m+1} \psi_{\xi,j}}\right] = \sum_{\xi=3}^{i} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} .$$

Тепер розглянемо другий доданок вираження (4.43) з урахуванням наступних співвідношень для вагових коефіцієнтів $V'_{i,j}$ і $V'_{2,j}$:

$$V'_{2,j} = \prod_{\xi=3}^{m+1} \psi_{\xi,j} , \; V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j} .$$

В цьому випадку отримаємо:

$$\left[\frac{a'_{2,j} V'_{2,j}}{V'_{i,j}}\right] = \left[\frac{a'_{2,j} \prod_{\xi=3}^{m+1} \psi_{\xi,j}}{\prod_{\xi=i+1}^{m+1} \psi_{\xi,j}}\right] = a'_{2,j} \prod_{\xi=3}^{i} \psi_{\xi,j} .$$

Перепишемо перший доданок вираження (4.43) з урахуванням наступних співвідношень для вагових коефіцієнтів $V'_{i,j}$ і $V'_{1,j}$:

$$V'_{1,j} = \prod_{\xi=2}^{m+1} \psi_{\xi,j}, \; V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}.$$

Тоді отримаємо:

$$\left[\frac{a'_{1,j} V'_{1,j}}{V'_{i,j}}\right] = \left[\frac{a'_{1,j} \prod_{\xi=2}^{m+1} \psi_{\xi,j}}{\prod_{\xi=i+1}^{m+1} \psi_{\xi,j}}\right] = a'_{1,j} \prod_{\xi=2}^{i} \psi_{\xi,j}.$$

Перепишемо перший доданок другій частині виразу (4.42) з урахуванням виконаних перетворень:

$$\left[\frac{a_{1,j} V'_{1,j}}{V'_{i,j}} + \frac{a'_{2,j} V'_{2,j}}{V'_{i,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j} V'_{i,j}}{V'_{i,j}}\right] =$$

$$= \left[a'_{1,j} \prod_{\xi=2}^{i} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=3}^{i} \psi_{\xi,j} + \sum_{\xi=3}^{i} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j}\right].$$

Тепер розглянемо другий доданок вираження (4.42):

$$\left[\frac{a_{1,j} V'_{1,j}}{\psi_{i,j} V'_{i,j}} + \frac{a'_{2,j} V'_{2,j}}{\psi_{i,j} V'_{i,j}} + \frac{\sum_{i=3}^{m+1} a_{i,j} V'_{i,j}}{\psi_{i,j} V'_{i,j}}\right] \cdot \psi_{i,j}. \qquad (4.45)$$

Перепишемо третій доданок вираження (4.45) з урахуванням наступного нерівності:

$$\psi_{i,j} V'_{i,j} > \sum_{i}^{m+1} a_{i,j} V'_{i,j}.$$

В цьому випадку отримаємо:

$$[\frac{\sum_{i=3}^{m+1} a_{i,j} V'_{i,j}}{\psi_{i,j} V'_{i,j}}] = [\frac{\sum_{\xi=3}^{i-1} a_{\xi,j} V_{\xi,j} + \sum_{\xi=i}^{m+1} a_{\xi,j} V'_{\xi,j}}{\psi_{i,j} V'_{i,j}}] = [\frac{\sum_{\xi=3}^{i-1} a_{\xi,j} V_{\xi,j}}{\psi_{i,j} V'_{i,j}}].$$

Перепишемо отримане вираз з урахуванням наступного співвідношення для вагового коефіцієнта $V'_{i,j}$:

$$V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}.$$

Тоді третій доданок вираження (4.45) прийме наступний вигляд:

$$[\frac{\sum_{\xi=3}^{i-1} a_{\xi,j} V_{\xi,j}}{\psi_{i,j} V'_{i,j}}] = [\frac{\sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{m+1} \psi_{\alpha,j}}{\psi_{i,j} \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}}] = \sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{i-1} \psi_{\alpha,j}$$

Тепер розглянемо другий доданок вираження (4.45) з урахуванням наступних співвідношень для вагових коефіцієнтів $V'_{2,j}$ і $V'_{i,j}$:

$$V'_{2,j} = \prod_{\xi=3}^{m+1} \psi_{\xi,j}, \; V'_{i,j} = \prod_{\xi=i+1}^{m+1} \psi_{\xi,j}.$$

В цьому випадку отримаємо:

$$[\frac{a'_{2,j}V'_{2,j}}{\psi_{i,j}V'_{i,j}}] = [\frac{a'_{2,j}\prod_{\xi=3}^{m+1}\psi_{\xi,j}}{\psi_{i,j}\prod_{\xi=i+1}^{m+1}\psi_{\xi,j}}] = a'_{2,j}\prod_{\xi=3}^{i-1}\psi_{\xi,j}.$$

Перепишемо перший доданок вираження (4.45) з урахуванням наступних співвідношень для вагових коефіцієнтів $V'_{i,j}$ і $V'_{1,j}$:

$$V'_{1,j} = \prod_{\xi=2}^{m+1}\psi_{\xi,j},\ V'_{i,j} = \prod_{\xi=i+1}^{m+1}\psi_{\xi,j}.$$

Тоді отримаємо:

$$[\frac{a'_{1,j}V'_{1,j}}{\psi_{i,j}V'_{i,j}}] = [\frac{a'_{1,j}\prod_{\xi=2}^{m+1}\psi_{\xi,j}}{\psi_{i,j}\prod_{\xi=i+1}^{m+1}\psi_{\xi,j}}] = a'_{1,j}\prod_{\xi=2}^{i-1}\psi_{\xi,j}.$$

Перепишемо другий доданок другій частині виразу (4.45) з урахуванням виконаних перетворень:

$$[\frac{a_{1,j}V'_{1,j}}{\psi_{i,j}V'_{i,j}} + \frac{a'_{2,j}V'_{2,j}}{\psi_{i,j}V'_{i,j}} + \frac{\sum_{i=3}^{m+1}a_{i,j}V'_{i,j}}{\psi_{i,j}V'_{i,j}}]\cdot\ \psi_{i,j} =$$

$$=[a'_{1,j}\prod_{\xi=2}^{i-1}\psi_{\xi,j} + a'_{2,j}\prod_{\xi=3}^{i-1}\psi_{\xi,j} + \sum_{\xi=3}^{i-1}a_{\xi,j}\prod_{\alpha=\xi+1}^{i-1}\psi_{\alpha,j}]\ \psi_{i,j}.$$

Розпишемо формулу (4.41) з урахуванням перетвореної правій частині виразу (4.42):

$$a^{*}_{i,j} = [a'_{1,j} \prod_{\xi=2}^{i} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=3}^{i} \psi_{\xi,j} + \sum_{\xi=3}^{i} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j}] -$$

$$-[a'_{1,j} \prod_{\xi=2}^{i-1} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=3}^{i-1} \psi_{\xi,j} + \sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{i-1} \psi_{\alpha,j}] \psi_{i,j} =$$

$$= a'_{1,j} \prod_{\xi=2}^{i} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=3}^{i} \psi_{\xi,j} + a_{i,j} + \sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} -$$

$$- a'_{1,j} \prod_{\xi=2}^{i} \psi_{\xi,j} + a'_{2,j} \prod_{\xi=3}^{i} \psi_{\xi,j} + \sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} =$$

$$= a_{i,j} + \sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} - \sum_{\xi=3}^{i-1} a_{\xi,j} \prod_{\alpha=\xi+1}^{i} \psi_{\alpha,j} = a_{i,j}$$

або

$$a^{*}_{i,j} = a_{i,j} .$$

Звідси відновлення елементів $a^{*}_{i,j}$ при авторизованому доступі здійснюється без внесення спотворень.

4.3 Приклад розробленого стеганографічного кодування

Тепер розглянемо приклад стеганографічного кодування, коли в число $A(j) = (3; 5; 2; 6)$ з нерівновагим базисом основ $\Psi^{(1)} = (7, 6, 6, 8)$ імплантується біт $a'_{2,j} = 1$ на позицію другого елементу. Тоді $A(j)'$ з імплантацією набуде вигляду:

$$A(j)' = (3; 1; 5; 2; 6).$$

У табл. 4.1 відображені проміжні значення величин, які використовувалися для отримання результуючої кодограми C'_j стеганокода $N(j)'$ числа $A'(j)$ з імплантацією, яка визначається за формулою:

$$C'_j = \{1728\}_2 + \{288\}_2 + \{240\}_2 + \{16\}_2 + \{6\}_2 = \{2278\}_2.$$

Другий рядок у табл. 4.1 містить значення для вбудованого елемента $a'_{2,j} = 1$. Значення для елементів числа $A(j)$ вихідної відеопослідовності містяться в інших рядках табл. 4.1.

довжина $q(j)'$ кодового представлення стеганокода $N(j)'$ числа $A(j)'$ з імплантованим елементом $a'_{2,j} = 1$ визначається на основі наступного виразу:

$$q(j)' = [\log_2 \psi_{1,j} + \log_2 \psi'_{2,j} \cdot + \ell og_2 (\prod_{i=3}^{m+1} \psi_{i,j})] + 1 = 12 \text{ (Біт)}.$$

Таблиця 4.1
Проміжні значення величин, для отримання кодограми C'_j.

i	$a_{i,j}$	$V'_{i,j}$	$a_{i,j}V'_{i,j}$	$C'_{i,j}$	$[\log_2 a_{i,j}V'_{i,j}]+1$	C'_j
1	3	576	1728	11011000000	11	2278
2′	1	288	288	100100000	9	
3	5	48	240	11110000	8	
4	2	8	16	10000	5	
5	6	1	6	110	3	

Для порівняння в табл. 4.2 наведені проміжні значення, які використовувалися для отримання кодограми стеганокода при встановленні на позицію першого елемента НПЧ.

З порівняльного аналізу табл. 4.1 і 4.2 можна зробити висновок, що:

а) значення стеганокода $N'_2(j)$ в разі вбудовування на позицію другого елементу НПЧ менше значення стеганокода $N'_1(j)$ при встановленні на позицію першого елемента;

б) значення $\Delta N_1(j)$ пульсації стеганокода при встановленні на позицію старшого елемента більше значення $\Delta N_2(j)$ пульсації стеганокода при встановленні на позицію другого елементу.

Іншими словами при формуванні стеганокода для числа з імплантацією на позиції другого елемента відбувається мінімізація внесених спотворень щодо значення коду-контейнера в порівнянні з стеганокодом для числа з імплантацією на позиції старшого першого елемента.

Таблиця 4.2
Проміжні значення величин, які використовуються при отриманні кодограми при встановленні на позицію першого елемента НПЧ.

i	$a_{i,j}$	$V'_{i,j}$	$a_{i,j}V'_{i,j}$	$C'_{i,j}$	$[\log_2 a_{i,j}V'_{i,j}]+1$	C'_j
1	1	2016	2016	11111100000	11	3142
2	3	288	864	1101100000	10	
3	5	48	240	11110000	8	
4	2	8	16	10000	5	
5	6	1	6	110	3	

Тепер оцінимо кількість $R_{стег}$ стеганографічної надмірності, яке вноситься в код-контейнер при встановленні на позицію другого елементу НПЧ. Величина $R_{стег}$ стеганографічної надмірності кодограми стеганокода $N(j)'$ числа $A(j)'$ щодо коду-контейнера $N(j)$ становить:

$$R_{стег} = q(j)' - q(j)'' = 12 - 11 = 1(\text{Біт}). \qquad (4.46)$$

Тут локалізація кількості $R_{стег}$ стеганографічної надмірності полягатиме в модифікації системи основ $\Psi^{(1)}$, а саме в збільшенні в два рази значення основи $\psi_{1,j}$ першого елемента $a_{1,j}$ нерівновагового позиційного числа, тобто:

$$\psi''_{1,j} = 2 \cdot \psi_{1,j}.$$

В цьому випадку, для правильного визначення неавторизованих користувачів довжини $q''(j)$ стеганокода $N(j)'$ буде виконуватися така умова:

$$q(j)'' = [\log_2 \psi''_{1,j} + \ell og_2(\prod_{i=2}^{m+1} \psi_{i,j})] + 1 =$$

$$= [\log_2 \psi_{1,j} + \log_2 \psi'_{2,j} + \ell og_2 (\prod_{i=2}^{m+1} \psi_{i,j})] + 1 = q(j)' .$$

Звідси, використання зловмисником скоригованої системи основ $\Psi'^{(1)}$ призводить до маскування структурної стеганографічної надмірності. В цьому випадку з огляду на вираз (4.46) кількість $R_{стег}$ структурної стеганографічної надмірності дорівнюватиме:

$$R_{стег} = q'(j) - q''(j) = 1 \text{ (Біт)}.$$

Але при неавторизований доступ зловмисник визначить довжину $q''(j)$ стеганокода $N(j)'$ з урахуванням скоригованого основи $\psi''_{1,j}$. При цьому кількість $R'_{стег}$ структурної стеганографічної надмірності щодо стеганокода $N(j)'$ дорівнюватиме нулю, тобто:

$$R'_{стег} = q'(j) - q''(j) = 0 \text{ (Біт)}.$$

Розглянемо процес формування кодограм для стеганокода при встановленні на позицію старшого і другого елементів нерівновагового позиційного числа.

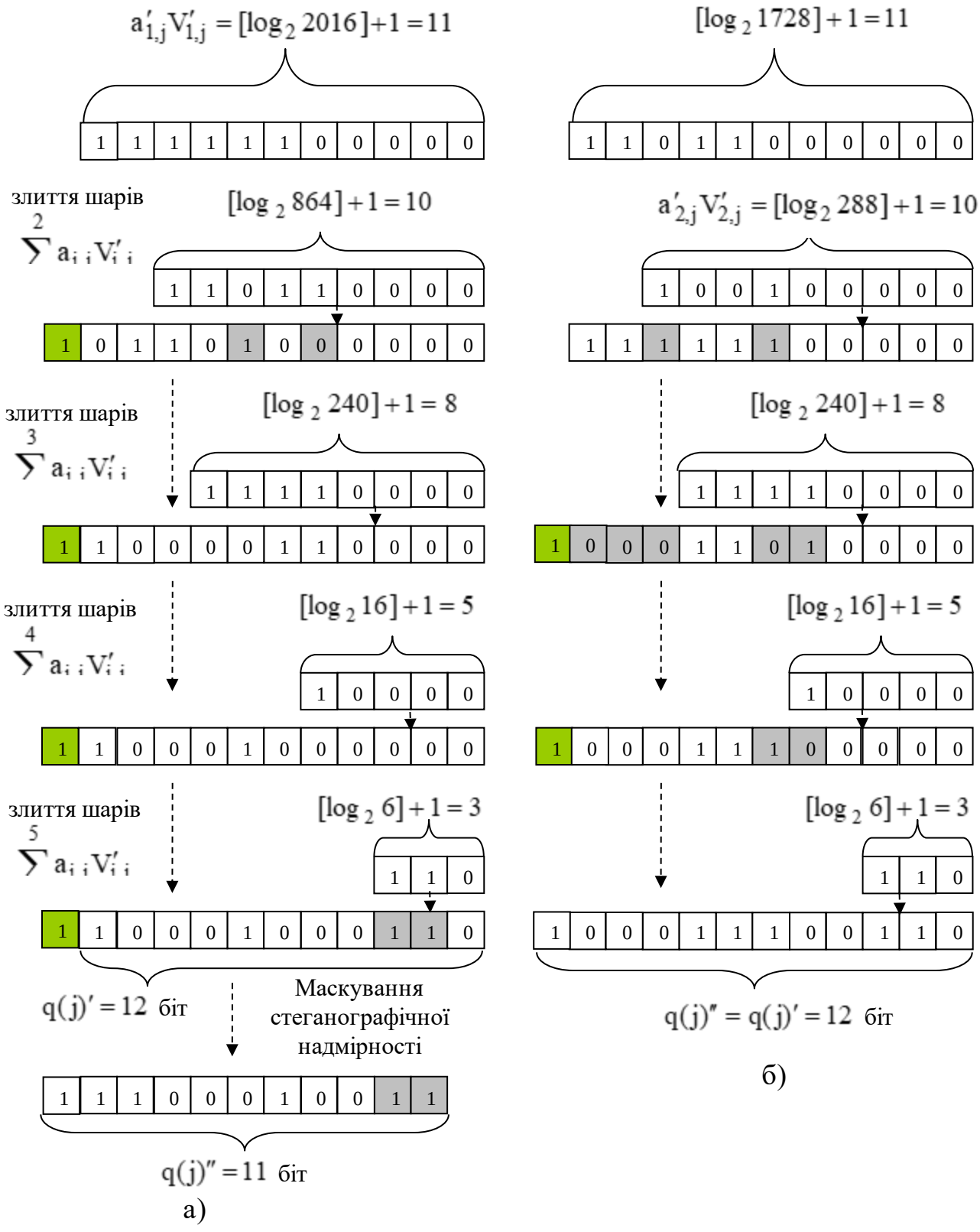

Рисунок 4.5 - Схема формування кодограми стеганокода для числа з імплантованим бітом на позицію першого (а) і другого (б) елементів НПЧ

На рисунку 4.5. відображений процес формування кодограми НП числа при імплантації біта на позиції першого а) і другого б) елементів НП числа. кодограми C'_j формується в результаті злиття нерівномірних бітових шарів $C_{i,j}$. тут значення і-го бітового шару $C_{i,j}$ визначається як двійкове подання твору елемента $a_{i,j}$ на його ваговий коефіцієнт $V'_{i,j}$, Тобто

$$C_{i,j} = [a_{i,j} V'_{i,j}]_2 .$$

У разі вбудовування біта $a'_{2,j} = 1$ процес стеганорафіческого кодування виключає корекцію кодограми стеганокода $N(j)'$. При цьому реконструкція елементів $a^*_{i,j}$ вихідної відеопослідовності в процесі стеганографічного декодування буде здійснюватися без внесення помилок [4].

Розглянемо процес стеганографічного декодування для авторизованого користувача. В цьому випадку відомі:

а) позиція стеганокода в стислому представленні зображення;

б) позиція вбудовування $\gamma = 2$;

в) основа $\psi'_{2,j} = 2$ вбудованого елемента $a'_{2,j} = 2$.

Розглянемо процес вилучення елемента $a''_{2,j}$ приховуваного повідомлення. Вилучення проводиться за формулою:

$$a''_{2,j} = [N(j)' / V'_{2,j}] - [N(j)' / (\psi'_{2j} V'_{2,j})] \ \psi'_{2,j} =$$
$$= [2278/288] - [2278/(2 \cdot 288)] \cdot 2 = 1 .$$

Звідки можна зробити висновок, що вбудований біт вилучається в процесі реконструкції без помилок, тобто:

$$a''_{1,j} = a'_{1,j} = 1.$$

Розглянемо тепер процес реконструкції елементів $a^*_{i,j}$ вихідної відеопослідовності

Відновлення першого елемента $a^*_{1,j}$ вихідної відеопослідовності здійснюється на основі модифікованого основи $\psi''_{1,j} = 2 \cdot \psi_{1,j} = 14$ за формулою (4.37):

$$a^*_{1,j} = [\ N(j)' / \ V_{1,j}\ ] - [\ N(j)' / (\psi''_{1,j}\, V_{i,j})\ ]\, \psi''_{1,j} =$$
$$= [\ 2278 \ / \ 576\ ] - [\, 2278 \ / (14 \cdot 576\,)] \cdot 14 = 3.$$

Відновлення інших елементів, $i = \overline{3, m+1}$ для вихідної відеопослідовності здійснюється за допомогою виразу (4.41).

для $i = 3$, значення елемента $a^*_{3,j}$ дорівнюватиме:

$$a^*_{3,j} = [2278 \ / \ 48] - [\, 2278 \ / (6 \cdot 48\,)] \cdot 6 = 5.$$

для $i = 4$, значення елемента $a^*_{4,j}$ дорівнюватиме:

$$a^*_{4,j} = [2278 \ / \ 8] - [\, 2278 \ / (6 \cdot 8\,)] \cdot 6 = 2.$$

для $i = 5$, значення елемента $a^*_{5,j}$ дорівнюватиме:

$$a^*_{i,j} = [2278 / 1] - [2278 \ / (8 \cdot 1\,)] \cdot 8 = 6.$$

В результаті демаскуючої стеганографічного декодування значення елементів $a^{*}_{i,j}$, реконструйованого числа $A(j)^{*}$ відновлені без помилок, тобто:

$$A(j)' = A(j)^{*}.$$

Тепер розглянемо процес відновлення елементів $a'''_{i,j}$ вихідної відеопослідовності при неавторизований доступ. В цьому випадку декодування буде здійснюватися на основі модифікованої системи основ $\Psi'^{(1)}$.

Відновлення першого елемента $a'''_{1,j}$ вихідної відеопослідовності здійснюється на основі модифікованого основи $\psi''_{1,j} = 2 \cdot \psi_{1,j} = 14$ за формулою (3.36):

$$a'''_{1,j} = [\ N(j)' / V''_{1,j}\ ] - [\ N(j)' / (\psi''_{1,j} V''_{i,j})\ ]\ \psi''_{1,j} =$$
$$= [2278 / 288] - [2278 / (14 \cdot 288)] \cdot 14 = 7.$$

Відновлення інших елементів, $i = \overline{2, m}$ для вихідної відеопослідовності здійснюється за допомогою виразу (3.49).

для $i = 2$, Значення елемента $a'''_{i,j}$ дорівнюватиме:

$$a'''_{2,j} = [2278 / 48] - [2278 / (6 \cdot 48)] \cdot 6 = 5.$$

для $i = 3$, Значення елемента $a'''_{i,j}$ дорівнюватиме:

$$a'''_{3,j} = [2278 / 8] - [2278 / (6 \cdot 8)] \cdot 6 = 2.$$

для $i = 4$, Значення елемента $a'''_{i,j}$ дорівнюватиме:

$$a'''_{4,j} = [2278 / 8] - [2278 / (8 \cdot 1)] \cdot 8 = 6.$$

В результаті декодування значень елементів $a'''_{i,j}$ реконструйованого числа $A'''(j)$ при неавторизований доступ значення елемента $a'''_{1,j}$ відновлено з помилкою, тобто

$$a'''_{1,j} \neq a_{1,j}.$$

значення інших $i = \overline{2,m}$ елементів $a'''_{i,j}$ відновлені без внесення помилок:

$$a'''_{i,j} = a_{i,j},\ i = \overline{2,m}.$$

5 ПРОГРАМНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОГО МЕТОДУ СТРУКТУРНО-СТЕГАНОГРАФІЧНОГО КОДУВАННЯ З ПЛАВАЮЧИХ БАЗИСОМ ВБУДОВУВАННЯ

5.1 Обгрунтування обраної мови програмування для написання додатку

Для написання програми була обрана зв’язка двух мов програмування, а саме Java та Kotlin.

Java - сильно типізована об'єктно-орієнтована мова програмування. Програми на Java транслюються в байт-код Java, який виконується віртуальною машиною Java (JVM) - програмою, яка виконує байтовий код і передає інструкції обладнанню як інтерпретатор.

Перевагою подібного способу виконання програм є повна незалежність байт-коду від операційної системи і устаткування, що дозволяє виконувати Java-додатки на будь-якому пристрої, для якого існує відповідна віртуальна машина. Іншою важливою особливістю технології Java є гнучка система безпеки, в рамках якої виконання програми повністю контролюється віртуальною машиною. Будь-які операції, які перевищують встановлені повноваження програми (наприклад, спроба несанкціонованого доступу до даних або з'єднання з іншим комп'ютером), викликають негайне переривання.

Kotlin (Котлін) - статично типізована мова програмування, що працює поверх JVM і розробляється компанією JetBrains. Автори ставили за мету створити мову більш лаконічну і типобезпечну, ніж Java, і більш просту, ніж Scala. Наслідком спрощення в порівнянні зі Scala стали також більш швидка компіляція і краща підтримка мови в IDE [5].

5.2 Реалізація алгоритму структурно-стеганографічного кодування використовуючи зображення у якості контейнера

Для реалізації прямого прямого стенаграфічного кодування була оновлена написанна функція OpcDirectWithMessageAt (рис. 5.1).

Першим аргументом вона приймає матрицю, яка виступає контейнером деякої ділянки зображення. Наступний аргумент – це контейнер для результату виконання функції, який містить у собі службову інформацію стосовно даної ділянки. Третій аргумент відповідає біту приховуваного повідомлення у даній ділянці. Останній аргумент відповідає позиції в поліадичному числі, у яку буде виконуватись вбудовування біту.

```
fun opcDirectWithMessageAt(
    dataOrigin: Matrix<Short>,
    dataOpc: DataOpc,
    message: Boolean,
    message_position: Int
) {
    var base = BigInteger.ONE
    for (i in dataOrigin.width - 1 downTo 0) {
        for (j in dataOrigin.height - 1 downTo 0) {
            if (dataOrigin[i, j].toInt() != 0) {
                dataOpc.N = dataOpc.N.add(base.multiply(BigInteger.valueOf(dataOrigin[i, j].toLong())))
            }
            base = base.multiply(BigInteger.valueOf(dataOpc.base[j].toLong()))

            if (i * dataOrigin.width + j == message_position) {
                if (message) dataOpc.N += base

                base *= TWO
            }
        }
    }
    dataOpc.base[0] = (dataOpc.base[0] * 2).toShort()
}
```

Рисунок 5.1 – Лістинг функції OpcDirectWithMessageAt

Функція за допомогою реверсивного обходу елементів матриці сегмента зображення формує поліадичну комбінацію для якої розраховує код та записує його у змінну N. Останньою операцією функція виконує процедуру маскування стенаграфічної надлишковості, яка полягає у збільшенні вдвічі основи старшого елементу.

У результаті виконання функії, контейнер містить у собі значення стеганокоду та службову інформацію, яка буде записана до файлу у двійковому вигляді на наступних етапах.

5.3 Реалізація алгоритму структурно-комбінаторного демаскуючого декодування

Для реалізації зворотнього перетворення була модифікована існуюча функція OpcReverceWithMessageAt (рис. 5.2).

```
fun opcReverseWithMessageAt(
    dataOrigin: Matrix<Short>,
    DataOpc: DataOpc,
    message_position: Int
): Boolean {
    var copy = BigInteger.ONE
    var b: BigInteger
    var message = false
    DataOpc.base[0] = (DataOpc.base[0] / 2).toShort()
    for (i in dataOrigin.width - 1 downTo 0) {
        for (j in dataOrigin.height - 1 downTo 0) {
            val a = DataOpc.N.divide(copy)
            val baseL = DataOpc.base[j].toLong()
            copy = copy.multiply(BigInteger.valueOf(baseL))

            b = DataOpc.N.divide(copy).multiply(BigInteger.valueOf(baseL))
            dataOrigin[i, j] = a.subtract(b).toShort()

            if (i * dataOrigin.width + j == message_position) {
                val tmp = (DataOpc.N / copy) - (DataOpc.N / (copy * TWO) * TWO)
                message = tmp.compareTo(BigInteger.ONE) == 0
                copy *= TWO
            }
        }
    }
    return message
}
```

Рисунок 5.2 – Лістинг функції OpcReverceWithMessageAt

Першим аргументом функції є матриця, у яку буде записана поліадична комбінація відповідна оригінальному сегменту зображення. Наступним аргументом функція отримує контейнер зі службовою інформацією та стеганокодом. Останнім аргументом функції є число вказуюче на передбачувану позицію вбудування біта приховуваного повідомлення.

Перед початком відтворення оригінальноі матриці, виконується зворотнє демаскуюче декодумання шляхом зменшення основи старшого елемента вдвічі

В результаті функція повертає значення прихованого біта, який використовується на наступних етапах для формування оригінального повідомлення.

6 ОЦІНКА ХАРАКТЕРИСТИК ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ РОЗРОБЛЕНОГО МЕТОДУ СТЕГАНОГРАФІЧНОГО КОДУВАННЯ

6.1 Заганьна оцінка розробленої стеганографічної системи

Розглянемо приклад використання розробленого стеганографічного методу для вбудовування прихованої інформації. В якості вихідних зображень використовуватимемо:

1) сильнонасичене зображення «Знімок аеропорту» (рис 6.1);

2) средньонасичене зображення «Лена» (рис 6.2).

Рисунок 6.1 - Зображення «Знімок аеропорту» - вихідне зображення-контейнер

Рисунок 6.2 - Зображення «Лена» - вихідне зображення-контейнер

Експеримент проводиться в наступних умовах:

а) початкові зображення можуть мати розмір всіх існуючих форматів, від нізкоформатних менше 0,1 Мпк до великоформатних зображень з роздільною здатністю більше 60 Мпк;

б) при встановленні інформації в зображення попереднього обліку структурних, статистичних та психовізуальних характеристик не проводиться, тобто виконується умова інваріантності щодо характеристик фрагментів, куди буде вбудована інформація;

в) щодо властивостей фрагментів зображення в процесі вбудовування інформації додаткових вимог не висувається, а саме забезпечується інваріантність щодо таких властивостей якості цифрових зображень як: колір, контрастність, насиченість, яскравість, ступінь когерентності;

г) в якості вихідних зображень для вбудовування допускається використання різних зображень за ступенем насиченості дрібними деталями і по їх походженню (реалістичні, штучні, змішані), тобто забезпечується

інваріантність щодо типу і класу зображень;

д) щодо приховуваного повідомлення попереднє перетворення не проводиться, тобто приховуване повідомлення вбудовується в вихідному двійковому поданні без попередніх трансформацій;

е) в процесі вбудовування на етапі імплантації довжина нерівноважних позиційних чисел вибирається рівної $m = 4$;

ж) імплантація одного біта інформації $b_\xi = 1$ здійснюється на другу позицію $\gamma = 2$ кожного нерівновагового позиційного числа:

$$A(j) = \{a_{1,j}; ...; a_{i,j}; ...; a_{m,j}\} \cup b_\xi = A'(j) = \{a_{1,j}; a'_{2,j} ...; a_{i,j}; ...; a_{m+1,j}\}.$$

Результати експерименту при неавторизований доступ представлені на основі декодованих зображень «Знімок аеропорту» (рис. 6.3) і «Лена» (рис. 6.4).

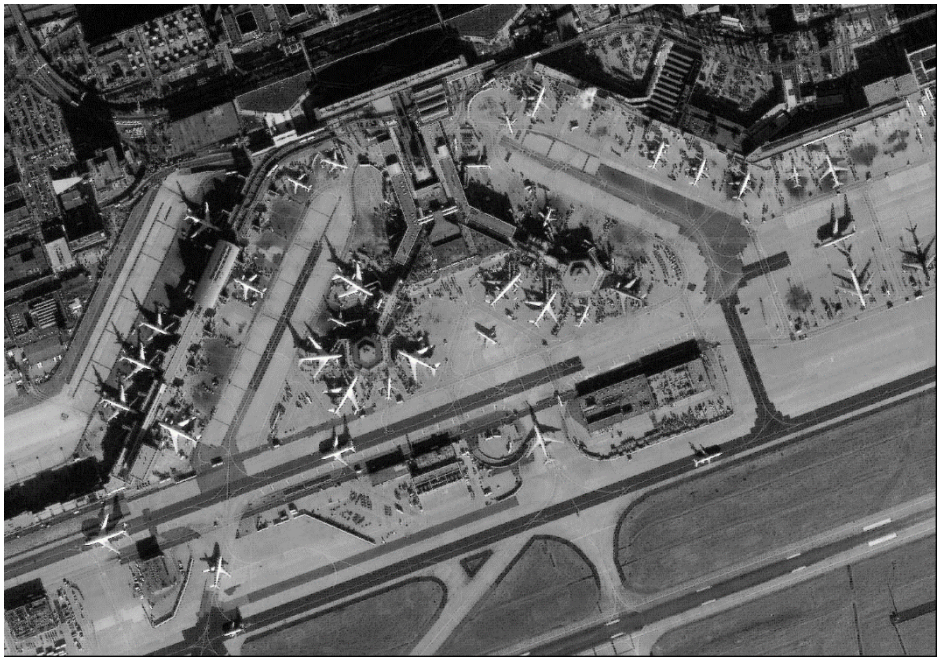

Рис 6.3. Зображення «Знімок аеропорту», декодоване неавториризованим користувачем

Рис 6.4. Зображення «Лена», декодоване неавториризованим користувачем

З аналізу зображень декодованих при неавторизованому доступі можна зробити висновок що:

1. Декодовані зображення «Знімок аеропорту» і «Лена» містять незначні візуальні спотворення. Такі спотворення виникають по контурах фрагментів декодованих зображень (рис 6.5. і рис. 6.6). Візуально, виявлені спотворення найбільш помітні в слабонасищенних областях зображення. У разі для сільнонасищенних зображення, такі спотворення помітні найменше. При неавторизований доступ в разі, коли противник не має вихідного зображення провести візуальну оцінку наявності вбудовування неможливо.

Рис 6.5. Маска стеганографічного вбудовування при неавторизований доступ для зображення «Знімок аеропорту»

Рис 6.6. Маска стеганографічного вбудовування при неавторизований доступ для зображення «Лена»

2. Значення пікового відношення сигнал-шум щодо вихідного зображення-контейнера становить: для зображення «Знімок аеропорту» -26 дБ, для зображення «Лена» - 27 дБ. Звідси, спостерігається збільшення значення пікового відношення сигнал шум щодо зображень декодованих неавторизованих користувачів в умовах вбудовування $b_\xi = 1$ на старшу позицію нерівновагового позиційного числа. Для зображень «Знімок аеропорту» і «Лена» значення пікового відношення сигнал-шум збільшується відповідно на 9 дБ і 13 дБ.

Спотворення, які з'явилися в процесі декодування, пояснюються впливом вбудовування на значення коду-контейнера. У цьому випадку значення коду-контейнера $N(j)$ збільшується на значення $\Delta N(j)$ пульсації стеганокода. Іншими словами зловмисник проводить декодування на основі значення стеганокода $N(j)'$, Яке відрізняється від значення коду-контейнера $N(j)$ на величину $\Delta N(j)$.

Реалізація демаскуючої стеганографічного декодування для авторизованого користувача розглядається на прикладі реконструкції зображень «Знімок аеропорту» і «Лена» представлених відповідно на рисунках 6.7 і 6.8.

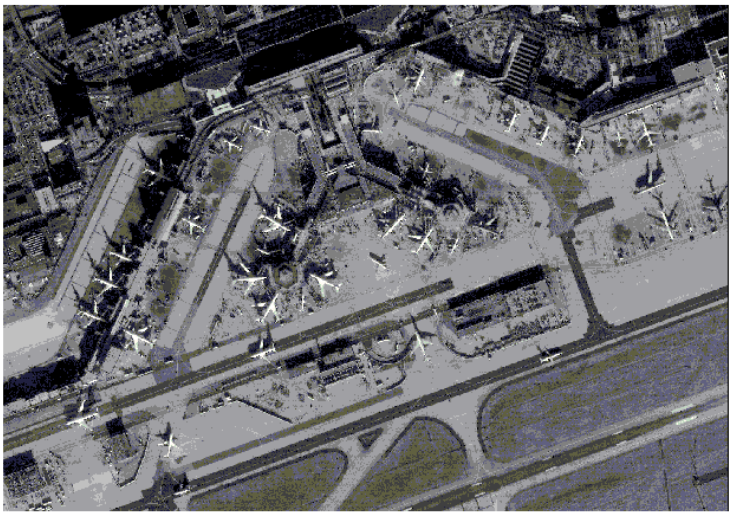

Рис 6.7. Зображення «Знімок аеропорту» отримане в результаті стеганографіч ного декодування для авторизованого користувача.

Рис 6.8. Зображення «Лена» - отримане в результаті стеганографічного декодування для авторизованого користувача

З аналізу зображень, отриманих в процесі стеганографічного декодування (авторизований доступ) можна зробити висновок наступне:

1. Вся вбудована інформація вилучається без помилок.

2. У реконструйованих зображеннях відсутні візуальні спотворення.

3. Середньоквадратичне відхилення для стеганографічно декодованих зображень «Знімок аеропорту» і «Лена» щодо вихідних зображень дорівнює нулю.

На основі проведених експериментів для розробленої стеганографічної системи можна зробити наступні висновки:

1. Відновлення вбудованої інформації при стеганографічному декодуванні для авторизованого користувача становить 100%.

2. Реконструйовані зображення при неавторизований доступ містять незначну кількість візуальних спотворень. У разі, коли противник не має вихідного зображення провести візуальну оцінку наявності вбудовування неможливо.

3. Розроблений стеганографічний метод дозволяє використовувати зображення, вилучені при стеганографічному декодуванні, в якості корисної інформації. В цьому випадку у відновленому оригінальному документі відсутні втрати.

4. Значення середньоквадратичного відхилення для стеганографічно декодованих зображень щодо вихідних зображень дорівнює нулю.

6.2 Оцінка стеганографічної ємності розробленої стеганографічної системи

Розроблений метод стеганографічного кодування дозволяє вбудовувати інформацію в цифрове зображення-контейнер на основі структурно-комбінаторних особливостей. Етапу стеганографічного кодування передує імплантація даних приховуваного повідомлення на позицію другого елементу нерівновагового позиційного числа $A(j)$ довжиною m. Множина нерівновагових позиційних чисел $\{A(j)\}$ довжиною m формується окремо для кожної кольорової складової зображення-контейнера [6].

Оцінку об'єму вбудовуваної інформації проводитимемо з позиції відносної стеганографічної ємності $w_{отн}^{(m)}$ системи.

Значення відносної стеганографічної ємності показує відсоткове відношення об'єму $w_{встр}^{(m)}$ вбудовуваної інформації відносно об'єму $W_{исх}$ зображення-контейнера. Дана величина використовується для оцінки ефективності стеганографічної системи за питомим обсягом вбудовуваної інформації відносно об'єму зображення-контейнера.

Діаграма залежності значення $w_{отн}^{(m)}$ відносної стеганографічної ємності стеганографічного алгоритму від різної довжини $m = 2; 3; 4; 6$ сформованих НЧ представлена на рис. 6.9.

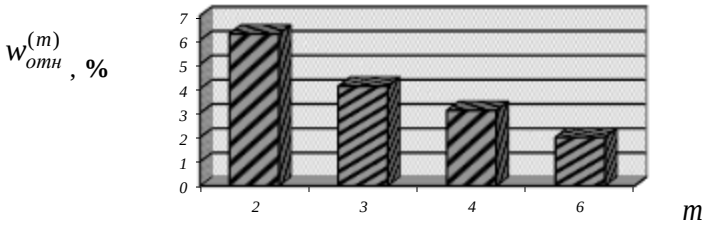

Рисунок 6.9 - Залежність значення $w_{отн}^{(m)}$ відносної стеганографічної ємності стеганографічного алгоритму від довжини m НПЧ

З аналізу рис. 6.9 можна зробити висновок, який полягає в тому, що в разі формування нерівновагового позиційного числа довжиною $m = 2$, відносна стеганографічна ємність розробленої системи набуває значення, рівного 6,25 %. Навпаки, при формуванні НПЧ довжиною $m = 6$ стеганографічна система володіє найменшою відносною ємністю -2%. Звідси витікає, що для забезпечення максимального значення відносної стеганографічної ємності при проектуванні стеганографічної системи на основі розробленого методу необхідно забезпечити формування нерівновагових позиційних чисел з найменшою довжиною в умовах досягнення необхідного рівня ефективного синтаксичного представлення.

Проведемо порівняльну оцінку відносної стеганографічної ємності $w_{отн}^{(m)}$ для розробленого стеганографічного методу і існуючих методів безпосереднього вбудовування інформації в зображення-контейнер. Порівняльну оцінку проводитимемо для наступних стеганографічних методів: метод вбудовування інформації в найменш значущий біт елементу спектрального представлення контейнера після квантування (режим 2 НЗБ); метод вбудовування інформації на основі розширення спектру (РС) [7].

У табл. 6.1 представлено значення відносної стеганографічної ємності методів НЗБ, РС і розробленого методу, а також значення пікового відношення сигнал-шум для зображень різної насиченості.

З аналізу оцінки відносної стеганографічної ємності в табл. 6.1 можна зробити наступні висновки:

а) при однакових значеннях відносної стеганографічної ємності виграш для розробленого методу відносно методу НЗБ в режимі 2 по величині пікового відношення сигнал-шум для різних класів зображень складає:

- для шагу квантування $q = 1$ від 6% до 66 %;

- для шагу квантування $q = 2$ від 35% до 75 %;

- для шагу квантування $q = 4$ від 47% до 80 %;

б) для розробленого методу виграш відносно методу РС по відносній стеганографічній ємності складає від 1,22 до 5,47 %, а по величині ПВСШ від 60 до 70% (що відповідає від 20 до 25 дБ).

Таблиця 6.1 - Залежність $w_{отн}^{(m)}$ значення від ПВСШ для зображень різної насиченості

Ємність %	Метод стеганографічного вбудовування		Значення ПВСШ, дБ		
			«Знімок аеропорту»	«Фотознімок»	«Літак на фоні неба»
6,25	НЗБ режим 2	$q = 1$	14,67	14,12	14,62
		$q = 2$	11,17	12,03	11,13
		$q = 4$	8,69	9,11	8,79
	РМ	$m = 2$	41,799	37,768	42,911
4,1	РМ	$m = 3$	39,074	35,058	40,052
3,1	НЗБ режим 2	$q = 1$	32,12	33,42	31,43
		$q = 2$	26,43	22,15	20,45
		$q = 4$	18,54	18,27	18,03
	РМ	$m = 4$	37,94	33,978	38,973
2	РМ	$m = 6$	36,931	33,019	38,121
0,78	РС	$\omega = 16$	16,93	13,019	18,121

6.3 Оцінка характеристик процесу приховання вбудованих повідомлень для неавторизованого доступу

Для розробленого стеганографічного методу вбудовування інформації на позицію старшого елементу нерівновагового позиційного числа оцінимо характеристики приховання вбудованих даних при неавторизованому доступі. В даному випадку така оцінка відповідатиме візуальній атаці противника, направленій на виявлення факту наявності вбудованої інформації. При цьому у противника буде відсутня наступна інформація: позиція вбудованого елементу $\gamma = 2$; основа вбудованого елементу $\psi'_\gamma = 2$.

Експериментально оцінимо візуальні характеристики процесу приховання даних для розробленого стеганографічного алгоритму. Експеримент проводиться в наступних умовах:

а) в процесі вбудовування на етапі імплантації довжина нерівновагових позиційних чисел вибирається рівною m=2;3;4;6;

б) імплантація одного біта інформації здійснюється на другу позицію $\gamma = 2$ кожного нерівновагового позиційного числа;

в) процес декодування здійснюється без усунення ефекту маскування (неавторизований доступ);

В якості вихідних зображень використовуватимемо (додаток «А»):

а) сильно насичене зображення «Знімок аеропорту»;

б) середньо насичене зображення «Фотознімок»;

в) слабо насичене зображення «Літак на фоні неба».

Результати експерименту в умовах вибору нерівновагового позиційного числа довжиною $m = 2$ представлені на прикладі наступних зображень, декодованих неавторизованим користувачем:

- сильно насичене декодоване зображення «Знімок аеропорту» (рис. 6.10)

Рисунок 6.10 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 2$

- середньо насичене декодоване зображення «Фотознімок» (рис. 6.11);

- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.12).

З аналізу зображень, декодованих при неавторизованому доступі можна зробити висновок, що значення пікового відношення сигнал шум розглянутих зображень відносно вихідних зображень-контейнерів складає:

- для сильно насиченого зображення «Знімок аеропорту» - 41,799 дБ;

- для середньо насиченого зображення «Фотознімок»- 37.768 дБ;
- для слабо насиченого зображення «Літак на фоні неба»- 42.911 дБ.

Рисунок 6.11 - Зображення «Фотознімок», декодоване неавторизованим користувачем при довжині НПЧ $m = 2$

Рисунок 6.12 - Зображення «Літак на фоні неба», декодоване неавторизованим користувачем при довжині НПЧ $m = 2$

Результати експериментів в умовах вибору нерівновагового позиційного числа довжиною $m = 3$ представлені на прикладі наступних зображень, декодованих при неавторизованому доступі:

- сильно насичене декодоване зображення «Знімок аеропорту» (рис. 6.13);
- середньо насичене декодоване зображення «Фотознімок» (рис. 6.13);
- слабо насичене декодоване зображення «Літак на фоні неба»

(рис. 6.14).

Рисунок 6.13 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 3$

Аналіз отриманих зображень показав, що величина пікового відношення сигнал-шум для декодованих зображень відносно вихідних зображень при неавторизованому доступі складає:

- для сильно насиченого зображення «Знімок аеропорту» - 39,074 дБ;
- для середньо насиченого зображення «Фотознімок» - 35,058 дБ;

Рисунок 6.14 - Зображення «Фотознімок», декодоване неавторизованим користувачем при довжині НПЧ $m = 3$

- для слабо насиченого зображення «Літак на фоні неба» - 40,052 дБ.

Тепер розглянемо результати експериментів в умовах вибору нерівновагового позиційного числа, довжиною $m = 4$. Результати представлені

на прикладі наступних зображень, декодованих при неавторизованому доступі:

- сильно насичене декодоване зображення «Знімок аеропорту» (рис. 6.16);
- середньо насичене декодоване зображення «Фотознімок» (рис. 6.17);
- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.18).

Рисунок 6.15 - Зображення «Літак на фоні неба», декодоване неавторизованим користувачем при довжині НПЧ $m = 3$

Рисунок 6.16 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 4$

З аналізу зображень виходить, що значення пікового відношення сигнал-шум для зображень, декодованих при неавторизованому доступі відносно вихідних зображень складає:

Рисунок 6.17 - Зображення «Фотознімок», декодоване неавторизованим користувачем при довжині НПЧ $m = 4$

Рисунок 6.18 - Зображення «Літак на фоні неба», декодоване неавторизованим користувачем при довжині НПЧ $m = 4$

- для сильно насиченого зображення «Знімок аеропорту» - 37,94 дБ;
- для середньо насиченого зображення «Фотознімок» - 33,978 дБ;
- для слабо насиченого зображення «Літак на фоні неба» - 38,973 дБ.

Наступний етап оцінки зображень, декодованих при неавторизованому доступі проводився в умовах вибору нерівновагового позиційного числа, довжиною $m = 6$. Результати оцінки представлені на прикладі наступних зображень:

- сильно насичене декодоване зображення «Знімок аеропорту» (рис. 6.19)

- середньо насичене декодоване зображення «Фотознімок» (рис. 6.20);

- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.21).

Рисунок 6.19 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 6$

Рисунок 6.20 - Зображення «Фотознімок», декодоване неавторизованим користувачем при довжині НПЧ $m = 6$

Рисунок 6.21 - Зображення «Літак на фоні неба», декодоване неавторизованим користувачем при довжині НПЧ $m = 6$

Проведений аналіз декодованих зображень показав, що значення пікового відношення сигнал шум для зображень, декодованих при неавторизованому доступі, відносно вихідних зображень-контейнерів складає:

- для сильно насиченого зображення «Знімок аеропорту» - 36,931 дБ;
- для середньо насиченого зображення «Фотознімок» - 33.019 дБ;
- для слабо насиченого зображення «Літак на фоні неба» - 38.121 дБ.

На рис. 6.22 представлені узагальнені результати за оцінкою значення пікового відношення сигнал-шум для декодованих зображень при неавторизованому доступі.

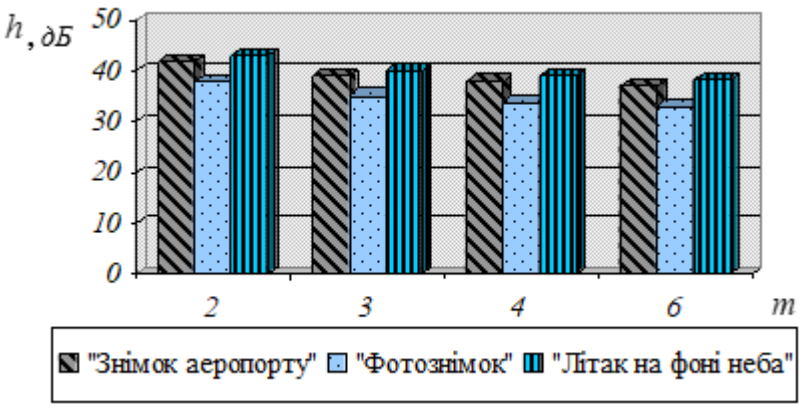

Рисунок 6.22 - Значення ПВСШ h для декодованих зображень при різних значеннях довжини m сформованих НПЧ

З аналізу рис. 6.22 можна зробити наступні висновки:

1. Для розробленого методу стеганографічного кодування візуальні спотворення, що вносяться до зображення при неавторизованому доступі, є незначними як з позиції зорового сприйняття, так і з позиції машинної обробки. Це дозволяє використовувати розроблений метод для прихованого вбудовування інформації.

2. За однакових умов стеганографічного кодування найбільші спотвореннями спостерігаються для реалістичних зображень з підвищеною яскравістю і середньою насиченістю дрібними деталями. Значення пікового

відношення сигнал-шум для середньо насиченого зображення «Фотознімок» менше значення пікового відношення сигнал-шум для сильно насиченого зображення «Знімок аеропорту» на 10-11 % (3,8-4 дБ). Значення ПВСШ для середньо насиченого зображення «Фотознімок» менше значення ПВСШ для сильно насиченого зображення «Літак на фоні неба» на 13 % (5 дБ).

3. Найкращою візуальною стійкість (найменшою уразливістю) до візуальної атаки, направленої на виявлення факту наявності вбудовування володіє розроблена стеганографічна система в разі вбудовування даних в слабо насичене зображення «Знімок літака на фоні неба». Для розробленого методу величина пікового відношення сигнал-шум для зображень, декодованих при неавторизованому доступі, для різних m набуває значень від 38.1 до 42.9 дБ.

4. Величина пікового відношення сигнал-шум для всіх типів зображення набуває найбільшого значення в разі вбудовування в нерівновагове позиційне число довжиною $m = 2$. При цьому виграш в значенні ПВСШ відносно вбудовування в НПЧ з довжиною $m = 3; 4; 6$ буде відповідно рівний:

- для сильно насиченого зображення «Знімок аеропорту» від 7 до 13%, що складає від 2,725 дБ до 4,86 дБ;

- для середньо насиченого зображення «Фотознімок» від 7 до 14%, що складає від 2,71 дБ до 4,79 дБ;

- для слабо насиченого зображення «Літак на фоні неба» від 7,1 до 12,5%, що складає від 2,85 дБ до 4,79 дБ.

Можна стверджувати, що враховуючи незначні зміни ПВСШ для декодованих зображень різної насиченості, в процесі проектування стеганографічної системи відсутня необхідність в попередній селекції контейнерів для вбудовування.

6.4 Порівняльна оцінка ефективності процесу вилучення приховуваної інформації авторизованим користувачем

Розглянемо процес вилучення стеганографічно вбудованих даних для розробленого методу. Необхідно враховувати, що для авторизованого користувача приховуване повідомлення є корисною інформацією. Тому при авторизованому доступі об'єм вилучених даних повинен складати 100 % від об'єму вбудованих даних [8]. Для розробленого методу, вилучення біта приховуваного повідомлення здійснюється за наявності наступної інформації (авторизований доступ):

- позиція стеганокоду в ефективному синтаксичному представленні зображення;
- позиція $\gamma = 2$ вбудованого елементу $a'_{1,j}$;
- основа $\psi'_{\gamma} = 2$ вбудованого елементу $a'_{1,j}$.

В цьому випадку демаскуюче стеганографічне декодування передбачає усунення ефекту локалізації структурної стеганографічної надлишковості. Проведення демаскування здійснюється шляхом ділення основи старшого елементу навпіл.

На рис. 6.23 представлена порівняльна діаграма значень ймовірності $P_{из}$ безпомилкового вилучення вбудованих даних для методів найменш значущого біта, розширення спектру і розробленого методу в умовах відсутності атак на вбудоване повідомлення.

З аналізу рисунка 6.23 можна зробити наступні висновки:

а) для розробленого стеганографічного методу ймовірність $P_{из}$ безпомилкового вилучення вбудованих даних в умовах відсутності атак на вбудоване повідомлення дорівнює одиниці;

б) виграш для розробленого методу відносно методу НЗБ за значенням ймовірності $P_{из}$ безпомилкового вилучення в умовах відсутності атак на

вбудоване повідомлення складає 40%;

в) виграш для розробленого методу відносно методу РС за значенням ймовірності $P_{из}$ безпомилкового вилучення в умовах відсутності атак на вбудоване повідомлення складає 50%;

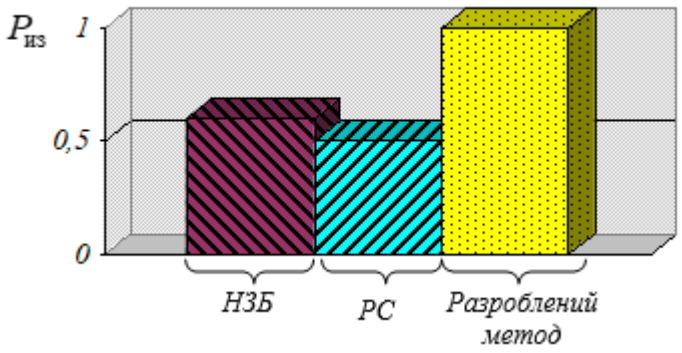

Рисунок 6.23 - Діаграма значень ймовірності $P_{из}$ для методів НЗБ, РС і розробленого методу в умовах відсутності атак на вбудоване повідомлення

г) виграш для розробленого методу відносно методу НЗБ за значенням ймовірності $P_{из}$ безпомилкового вилучення в умовах відсутності атак на вбудоване повідомлення складає 40%;

д) виграш для розробленого методу відносно методу РС за значенням ймовірності $P_{из}$ безпомилкового вилучення в умовах відсутності атак на вбудоване повідомлення складає 50%;

е) наявність для розробленого методу можливості безпомилкового вилучення вбудованих даних в умовах відсутності атак дозволяє використовувати його для успішного приховання інформації в кризових системах.

6.5 Оцінка стійкості приховуваних повідомлень до атак зловмисника для розробленої стеганографічної системи

Оцінимо стійкість процесу вбудовування даних на основі розробленого стеганографічного кодування в умовах застосування противником активної атаки, направленої на руйнування вбудованого повідомлення [9].

Така оцінка передбачає перевірку ефективності використання розробленого стеганографічного алгоритму в умовах застосування зловмисником наступних атак:

1. Виконання прямого і зворотнього дискретного косинусного перетворення з подальшим округленням (речовинного) значення.

2. Пряме і зворотнє квантування з різними чинниками втрати якості.

Атакам піддаються значення стеганокодів, сформованих для зображень різних типів, а саме:

а) сильно насичене зображення «Знімок аеропорту»;

б) середньо насичене зображення «Фотознімок»;

в) слабо насичене зображення «Знімок літака на фоні неба».

Експеримент проводиться в наступних умовах:

а) в процесі вбудовування на етапі імплантації довжина нерівновагових позиційних чисел вибирається рівною m=2;3;4;6;

б) формування нерівновагових позиційних чисел проводиться для трьох колірних компонентів досліджуваного зображення;

в) імплантація одного біта інформації здійснюється на другу позицію $\gamma = 2$ кожного нерівновагового позиційного числа, тобто:

$$A(j) = \{a_{1,j}; ...; a_{i,j}; ...; a_{m,j}\} \cup b_{\xi} = \\ = A'(j) = \{a_{1,j}; a'_{2,j} ...; a_{i,j}; ...; a_{m+1,j}\}; \quad (6.1)$$

г) значення коефіцієнта квантування вибирається рівним q=1;2;5;10.

Таблиця 6.2 Відсоткове співвідношення $w_{из}^{(m)}$ безпомилково вилучених бітів вбудованого повідомлення для зображення «Знімок аеропорту» в умовах атак

Умови атаки	Кількість $w_{из}^{(m)}$ безпомилково вилучених бітів вбудованого повідомлення %			
	$m = 2$	$m = 3$	$m = 4$	$m = 6$
Без атаки	100	100	100	100
ДКП	98,3	99,3	99,7	99,9
$q = 1$	80,4	91,9	96,8	99,4
$q = 2$	78,5	91	96,4	99,3
$q = 5$	75,6	90	95,9	99,3
$q = 10$	74,1	89,1	95,4	99,2

У табл. 6.2 представлені значення відсоткового співвідношення кількості $w_{из}^{(m)}$ безпомилково вилучених біт відносно кількості $w_{встр}^{(m)}$ вбудованих біт для розробленої стеганографічної системи в умовах атак.

Проаналізувавши значення в табл. 6.2 можна зробити висновок, що:

а) для розробленого стеганографічного кодування кількість $w_{из}^{(m)}$ безпомилково вилучених даних в умовах відсутності активних атак набуває значення 100% незалежно від довжини сформованих нерівновагових позиційних чисел;

б) для розробленого методу в умовах атаки дискретного косинусного перетворення з квантуванням, з шагом $q = 10$ найменший відсоток 74,1 % по кількості $w_{из}^{(m)}$ правильно вилучених біт досягається для повідомлення вбудованого в нерівновагове позиційне число, довжиною $m = 2$;

в) найбільший відсоток 99,2 % по кількості $w_{из}^{(m)}$ правильно вилучених бітів в умовах атаки ДКП і квантування з шагом $q = 10$ для розробленого методу досягається для стеганографічно вбудованого повідомлення в нерівновагове позиційне число довжиною $m = 6$.

У табл. 6.3 представлені відсоткові значення $w_{из}^{(m)}$ кількості безпомилково вилучених бітів стеганографічно вбудованого повідомлення в

зображення «Фотознімок» в умовах атак.

Проаналізувавши значення в табл. 6.3 можна зробити висновок, що:

а) для розробленого стеганографічного кодування кількість $w_{из}^{(m)}$ безпомилково вилучених даних в умовах відсутності активних атак набуває значення 100% незалежно від довжини сформованих нерівновагових позиційних чисел;

б) для розробленого методу в умовах атаки ДКП і квантування з шагом $q = 10$ найменший відсоток 72,9 % по кількості $w_{из}^{(m)}$ правильно вилучених біт досягається для повідомлення, стеганографічно вбудованого в НПЧ довжиною $m = 2$;

в) для розробленого методу в умовах атаки ДКП і квантування з шагом $q = 10$ найменший відсоток 72,9 % по кількості $w_{из}^{(m)}$ правильно вилучених біт досягається для повідомлення, стеганографічно вбудованого в НПЧ довжиною $m = 2$;

Таблиця 6.3 Відсоткове співвідношення $w_{\text{вост}}$ безпомилково вилучених бітів вбудованого повідомлення для зображення «Фотознімок»

Умови атаки	Кількість $w_{из}^{(m)}$ безпомилково вилучених бітів вбудованого повідомлення %			
	$m = 2$	$m = 3$	$m = 4$	$m = 6$
Без атаки	100	100	100	100
ДКП	98	99,1	99,9	99,9
$q = 1$	76,9	89,4	94,2	98,3
$q = 2$	75,2	88,4	93,8	98,3
$q = 5$	73,4	87,4	93,3	98,2
$q = 10$	72,9	87,2	93,1	98,2

г) для розробленого методу в умовах атаки ДКП і квантування з шагом $q = 10$ найменший відсоток 72,9 % по кількості $w_{из}^{(m)}$ правильно вилучених бітів досягається для повідомлення, стеганографічно вбудованого в НПЧ довжиною $m = 2$;

д) найбільший відсоток 98,2 % по кількості $w_{из}^{(m)}$ правильно вилучених біт в умовах атаки ДКП і квантування з шагом $q = 10$ для розробленого методу досягається при вбудовуванні повідомлення в нерівновагове позиційне число, довжиною $m = 6$.

У табл. 6.4 представлено відсоткові значення $w_{из}^{(m)}$ кількості безпомилково вилучених бітів стеганографічно вбудованого повідомлення в зображення «Літак на фоні неба» в умовах атак.

Проаналізувавши значення в табл. 6.4 можна зробити висновок, що:

а) для розробленого стеганографічного кодування кількість $w_{из}^{(m)}$ безпомилково вилучених даних в умовах відсутності активних атак набуває значення 100% незалежно від довжини сформованих нерівновагових позиційних чисел;

Таблиця 6.4 Відсоткове співвідношення $\boldsymbol{w_{из}^{(m)}}$ безпомилково вилучених бітів вбудованого повідомлення для зображення «Літак на фоні неба» в умовах атак

Умови атаки	Кількість $w_{из}^{(m)}$ безпомилково вилучених бітів вбудованого повідомлення %			
	$m = 2$	$m = 3$	$m = 4$	$m = 6$
Без атаки	100	100	100	100
ДКП	97,7	99,2	99,7	99,9
$q = 1$	78,2	89,8	97,2	99,8
$q = 2$	74,6	89,1	96,9	99,8
$q = 5$	69,6	88,1	96,6	99,7
$q = 10$	68,7	87,8	96,5	99,8

б) для розробленого методу в умовах атаки ДКП і квантування з шагом $q = 10$ найменший відсоток 68,7 % по кількості $w_{из}^{(m)}$ правильно вилучених бітів досягається для стеганографічно вбудованого повідомлення в НПЧ довжиною $m = 2$;

в) в умовах атаки ДКП і квантування з шагом $q = 10$ найменший відсоток

99,8 % по кількості $w_{из}^{(m)}$ правильно вилучених бітів досягається для повідомлення вбудованого на основі розробленого методу в НПЧ довжиною $m = 6$.

Порівняємо відсоткові значення кількості $w_{из}^{(z_{стр} z_{стб})}$ вилучених бітів відносно кількості $w_{встр}^{(z_{стр} z_{стб})}$ вбудованих бітів для методу розширення спектру, найменш значущого біта і розробленого методу.

Для методу НЗБ і РС кількість $w_{из}^{(z_{стр} z_{стб})}$ безпомилково вилучених бітів в умовах активних атак складає 50%.

На рис. 6.24 представлена діаграма відсоткового значення кількості безпомилково вилучених бітів для методів НЗБ, РС і розробленого методу в умовах застосування атаки ДКП і квантування з шагом $q = 0; 1; 5$.

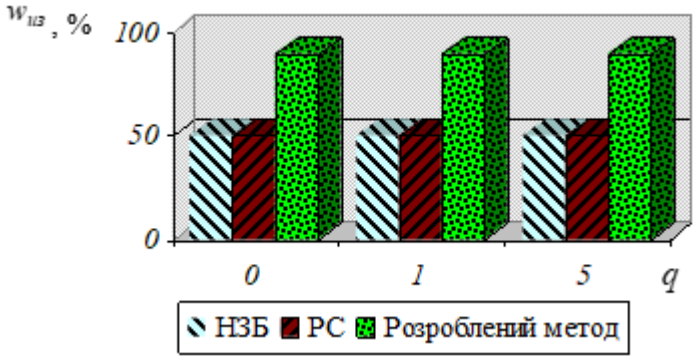

Рисунок 6.24 - Діаграма значень величини $w_{из}^{(m)}$ для методу НЗБ, РС і розробленого методу залежно від типу атак

З аналізу рис. 6.24 можна зробити наступні висновки:

а) для досліджуваних значень коефіцієнтів квантування кількість $w_{из}^{(m)}$ безпомилково вилучених бітів для розробленого методу набуває значень не менше 90 %;

б) в умовах застосування активних атак виграш для розробленого методу відносно методів НЗБ і РС по кількості безпомилково вилучених даних складає 40 %.

6.6 Оцінка стеганографічного бітрейта розробленої стеганографічної системи

Для розробленої системи безпосереднього вбудовування оцінимо величину стеганографічного бітрейта, який визначається на основі наступного виразу:

$$S_b = \lim_{\substack{P_{из}\to 1 \\ h\to\infty}} (f(w_{встр}, Z_{стр} Z_{стб}, P_{из}, h)), \qquad (6.2)$$

де $f(\bullet)$ - функціональне перетворення, яке використовується для визначення стеганографічного бітрейта;

$w_{встр}$ - величина абсолютної стеганографічної ємності, тобто максимальний об'єм повідомлення, яке можна вбудувати в зображення, вимірюється в бітах;

$Z_{стр} Z_{стб}$ - мінімально необхідний розмір зображення, достатній для вбудовування інформації об'ємом $w_{встр}$ на основі оцінюваного стеганографічного алгоритму;

$P_{из}$ - ймовірність безпомилкового вилучення вбудованих даних;

h - величина пікового відношення сигнал-шум.

Фізичний зміст стеганографічного бітрейта S_b полягає в тому, що дана величина характеризує кількість пікселів, яка необхідна для вбудовування одного біта приховуваного повідомлення. Стеганографічний бітрейт вимірюється в бітах на піксель (біт/піксель). На практиці використовується наступний вираз для визначення стеганографічного бітрейта:

$$S_b = \frac{w_{встр}}{Z_{стр} Z_{стб}}, \qquad (6.3)$$

де $w_{встр}$ - величина абсолютної стеганографічної ємності, тобто максимальний об'єм повідомлення, яке можна вбудувати в зображення, вимірюється в бітах;

$Z_{стр}Z_{стб}$ - мінімально необхідний розмір зображення, достатній для вбудовування інформації об'ємом $w_{встр}$ на основі оцінюваного стеганографічного алгоритму.

На рис. 6.25 представлена діаграма залежності величини $S_b^{(m)}$ стеганографічного бітрейта розробленої стеганографічної системи від різної довжини m=2;3;4;6 сформованих нерівновагових позиційних чисел.

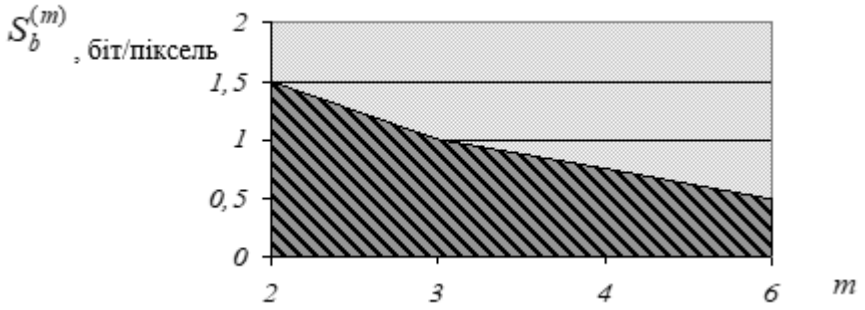

Рисунок 6.25 - Залежність величини $S_b^{(m)}$ стеганографічного бітрейта розробленого методу від довжини m НПЧ

З аналізу діаграми на рис. 6.25 можна зробити висновок, який полягає в тому, що в разі формування нерівновагового позиційного числа довжиною $m=2$, величина $S_b^{(m)}$ пропускної спроможності розробленої системи набуває найбільшого значення, рівного 1,5 біт на піксель. Навпаки, при формуванні НПЧ довжиною $m=6$ стеганографічна система володіє найменшою пропускною спроможністю – 0,5 біт на піксель.

На рис. 6.26 – 6.28 представлені діаграми залежності величини S_b значення і величини h пікового відношення сигнал шум зображень різною насиченістю для методів найменш значимого біта, розширення спектру і

розробленого методу.

З аналізу діаграм на рис. 6.26 – 6.28 можна зробити наступні висновки:

а) для розробленого методу найбільшого значення стеганографічний бітрейт набуває в разі формування нерівновагових позиційних чисел довжиною $m=2$ - 1,5 біта на піксель, і навпаки найменше значення величини S_b спостерігається для нерівновагових позиційних чисел довжиною $m=6$ - 0,5 біта на піксель;

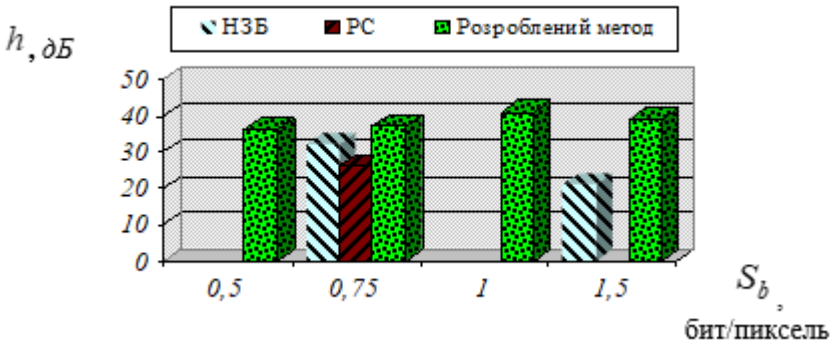

Рисунок 6.26 - Діаграма значень величини S_b і h для сильно насиченого зображення, декодованого на основі методу НЗБ, РС і розробленого методу

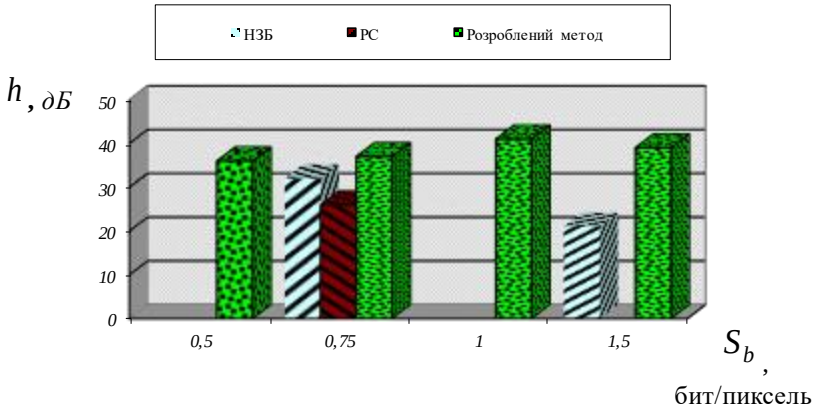

Рисунок 6.27 - Діаграма значень величини S_b і h для середньо насиченого зображення, декодованого на основі методу НЗБ, РС і розробленого методу

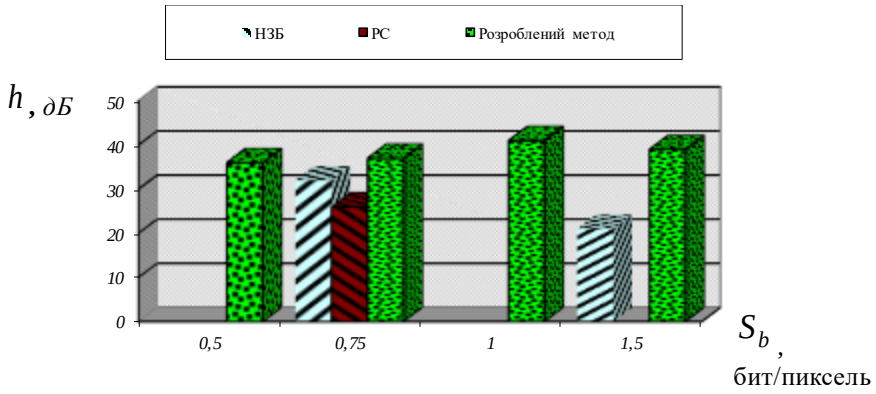

Рисунок 6.28 - Діаграма значень величини S_b і h для слабо насиченого зображення, декодованого на основі методу НЗБ, РС і розробленого методу

З аналізу діаграм на рис. 6.26 – 6.28. можна зробити наступні висновки:

а) для розробленого методу найбільшого значення стеганографічний бітрейт набуває в разі формування нерівновагових позиційних чисел довжиною $m = 2$ - 1,5 біта на піксель, і навпаки найменше значення величини S_b спостерігається для нерівновагових позиційних чисел довжиною $m = 6$ - 0,5 біта на піксель;

б) виграш для розробленого методу відносно методу НЗБ і РС по величині стеганографічного бітрейта:

-для методу НЗБ в середньому до 25 %;

- для методу РС в середньому до 25 %.

ВИСНОВКИ

1. Обґрунтовано недоліки стеганографічної системи на основі вбудовування приховуваного елемента на першу позицію нерівновагового позиційного числа. Усунення структурної стеганографічної надмірності в разі такого стеганографічного перетворення здійснюється на основі корекції кодограми стеганокода шляхом відсікання молодшого значущого біта. Таке коригування призводить до виникнення залишкових спотворень в разі реконструкції зображення зловмисником. У разі авторизованого доступу процес демаскування структурної стеганографічної надмірності здійснюється шляхом додавання нульового біта в скориговане значення кодограми. Це створює умови для того що не всі елементи відновленого позиційного числа будуть збігатися з елементами нерівновагового позиційного числа вихідної відеопослідовності.

- знижує ефективність приховування вбудовується інформації;

- знижує якість вихідних зображень.

2. Запропоновано підхід у вигляді локалізації структурної стеганографічної надмірності не пов'язана з корекцією кодограми стеганокода. Організація такої локалізації здійснюється шляхом модифікації нерівновагового позиційного базису, а саме окремих основ елементів нерівновагового позиційного числа. Обґрунтовано підхід при виборі позиції елемента НПЧ, для якого буде проводитися коригування основ.

Доведена теорема безпохибкового вилучення вбудованої інформації. При цьому позиція елемента з модифікованою основою повинна бути старше позиції вбудованого елемента.

У той же час для мінімізації спотворень, що вносяться до стеганокоду убудовуванням елемента, обґрунтовано необхідність зменшення позиції вбудовування елемента приховуваного повідомлення.

Наукова новизна: Вперше запропоновано підхід для локалізації

структурної стеганографічної надлишковості на основі модифікації системи основ. Це дозволяє здійснювати маскування структурної стеганографічної надлишковості, що не пов'язане з корекції кодограми стеганокода. При цьому позиція елемента з модифікованою основою повинна бути старше позиції вбудовування.

3. Створено правило вбудовування інформації для структурного стеганографічного кодування, що полягає в тому, що:

а) один біт приховуваного повідомлення вбудовується на другу позицію нерівновагового позиційного числа;

б) модифікації піддається основа першого елемента, шляхом збільшення її в два рази.

Використання даного правила в процесі побудови стеганографічного кодування забезпечує:

а) вирівнювання довжини кодограми коду-контейнера щодо довжини кодограми стеганокода;

б) відновлення елемента приховуваного повідомлення без втрат;

в) мінімізацію спотворень внесених в вихідне зображення

На основі правила побудовано стеганографічне кодування з модифікацією системи основ для вбудовування одного біта на позицію другого елементу нерівновагового позиційного числа. Це забезпечує вбудовування прихованої інформації в умовах:

а) відсутності корекції кодограми стеганокода;

б) зниження кількості внесених спотворень в стеганокод;

в) забезпечення стійкості вбудованої інформації.

Наукова новизна. Вперше розроблено структурне стеганографічне кодування на основі імплантації біта приховуваного повідомлення на позицію другого елементу НПЧ з модифікацією нерівновагового позиційного базису. На відміну від інших методів забезпечується локалізація структурної стеганографічної надлишковості без внесення спотворень в кодограми стеганокода. Це дозволяє знизити можливість виявлення зловмисником факту

наявності вбудованої інформації (локалізувати атаку виявлення факту наявності вбудованої інформації).

4. Розроблено стеганографічне декодування для вилучення імплантованого на другу позицію біта з одночасною реконструкцією елементів вихідного нерівноважного позиційного числа. Процес декодування не передбачає усунення локалізації структурної стеганографічної надлишковості. Декодування включає наступні етапи:

а) структурний – стеганографічне декодування, що забезпечує відновлення нерівновагового позиційного числа з імплантованим елементом;

б) вилучення елемента приховуваного повідомлення з другої позиції нерівновагового позиційного числа;

в) відновлення значення нерівновагового позиційного числа вихідної відеопослідовності без внесення помилок.

Наукова новизна. Вперше розроблено стеганографічне декодування без усунення локалізації структурної стеганографічної надлишковості. На відміну від існуючих методів вилучення приховуваної інформації і відновлення нерівновагового позиційного числа проводиться на основі реконструкції стеганокода за біполярним принципом без демаскування стеганографічної надлишковості. Це дозволяє підвищити ефективність вилучення приховуваної інформації та локалізацію атаки зловмисника щодо виявлення факту наявності прихованої інформації.

5. Проведено експерименти з обробки насичених реалістичних зображень з використанням розробленої стеганографічної системи для вбудовування інформації на позицію другого елементу нерівновагового позиційного числа. В результаті чого отримані такі результати:

а) 100% вбудованої інформації витягується без помилок;

б) для декодованих зображень при неавторизованому доступі зменшується кількість візуальних спотворень щодо декодованих зображень при встановленні на позицію старшого елемента НПЧ, а пікове відношення сигнал-шум для зображень «Знімок аеропорту» і «Лена» збільшується в

порівнянні з такими ж зображеннями, стеганографічно декодуванним при встановленні на позицію старшого елемента, на 9 дБ і 11 дБ відповідно;

в) виявлені при неавторизованому доступі спотворення виникають по контурах фрагментів декодованих зображень, такі спотворення найбільш помітні в слабонасиченних областях зображення, і найменше помітні в сильнонасиченних зображеннях;

г) при неавторизованому доступі, в разі коли противник не має вихідного зображення, проведення візуальної оцінки наявності вбудовування, неможливо;

д) при авторизованому доступі зображення відновлюються без помилок і в разі необхідності можуть бути використані як корисна інформація;

е) при авторизованому доступі середньоквадратичне відхилення для стеганографічно декодованих і «Знімок аеропорту» і «Лена» дорівнює нулю, тобто реконструкція зображень здійснюється без внесення помилок;

Отримані наукові результати є внеском у розвиток теорії інформаційної безпеки відносно забезпечення безпеки спеціальних інформаційних ресурсів в кризових системах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Аграновски А.В. Стеганография, цифровые водяные знаки и стегоанализ [Тест]: учеб. пособие для вузов / А.В. Аграновски, А.В. Балакин, В.Г. Грибунин. – М.:Вузовская книга, 2009. – 220 с.

2. Алфёров А. П. Основы криптографии: учебное пособие / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

3. Андреев А. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 7. – С.19 – 25.

4. Андреев А.. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 8. – С.16 – 22.

5. Анин Б. Защита компьютерной информации / Б.Анин. - СПб.: БХВ-Петербург, 2000. - 384 с.

6. Артехин Б.В. Стеганография / Артехин Б.В. // Журнал «Защита информации. Конфидент». – 1996. - № 4 -

7. Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький // Системи обробки інформації : зб. наук. праць. – № 9 (107). – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 163–168.

8. Баранник Д.В. Концепция структурного стеганографического кодирования с маскированием / Д.В. Баранник, А.Э. Бекиров // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 4 - 11.

9. Баранник Д.В. Стеганографическая система на основе неравновестного позиционного кодирования / Д.В. Баранник, В.В. Баранник, А.Э. Бекиров // Радіоелектроніка та інформатика. - 2014. - №4. - С. 37 – 46.

ПЕРЕЛІК ПУБЛІКАЦІЙ

1. A steganographic method based on the modification of regions of the image with different saturation [Текст]: / Д. В. Бараннік[и др.] // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference.— 2018— С. 542-545.

2.The video stream encoding method in infocommunication systems [Текст]: / Д. В. Бараннік[и др.] // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference.— 2018— С. 538-541.

3. The information integrity enhance in telecommunication systems with the binomial coding [Текст]:/ Д. В. Бараннік[и др.] // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International.— 2017— С. 547-550.

4. The new method of secure data transmission on the indirect steganography basis [Текст]: / Д. В. Бараннік[и др.] // East-West Design & Test Symposium (EWDTS), 2016 IEEE.— 2016— С. 1-4.

5. Analyzing the ways of matching dynamic features of video stream to information and communication networks [Текст]: / Д. В. Бараннік[и др.] Kharkiv National University of Radio Electronics.— 2016.

6. Method of ciphergrams coding for increasing the effectiveness of technologies of selective cyber-protection [Текст]: / Д. В. Бараннік[и др.] // Kharkiv National University of Radio Electronics.— 2016.

7. Метод снижения информационной интенсивности достаточно информативных сегментов аэрофотоснимка [Текст]: / Д. В. Бараннік[и др.] // Харьковский национальный университет радиоэлектроники.— 2018.

8. Метод криптосемантичного представлення зображень на основі плаваючої схеми системи поліадичного кодування в диференціальному базисі [Текст]: / Д. В. Бараннік[и др.] // Наукоємні технології // 33.1— 2017- С. 46-52.

9. Метод кодування ресурсних блоків для технології 5G [Текст]: / Д. В. Бараннік[и др.] // Наукоємні технології // 37.1— 2018.

10. Технология балансированной обработки динамического видеоресурса для снижения информационной интенсивности в инфокоммуникационных системах [Текст]: / Д. В. Бараннік[и др.] // Безпека інформації // 23.3.— 2018 – С. 163-170.

11. Метод криптокомпрессионного представления изображений на основе двухкаскадного обобщенного позиционного кодирования в базисе по верхним [Текст]: / Д. В. Бараннік[и др.] //Радиоэлектроника и информатика // 1 - Харьковский национальный университет радиоэлектроники.— 2017.

12. Метод локализации потери целостности информации на основе слот-технологии [Текст]: / Д. В. Бараннік[и др.] // Радиоэлектроника и информатика // 4 - Харьковский национальный университет радиоэлектроники.— 2015.

13. Обоснование подхода для формирования квантованного описания трансформанты сегмента аэрофотоснимка [Текст]: / Д. В. Бараннік[и др.] // Автоматизированные системы управления и приборы автоматики // 173 - Харьковский национальный университет радиоэлектроники.— 2015.

14. Стеганографическая система на основе нерівновагового позиционного кодирования [Текст]: / Д. В. Бараннік[и др.] // Радиоэлектроника и информатика // 4 - Харьковский национальный университет радиоэлектроники.— 2014.

15. Концепция структурного стеганографического кодирования с маскированием [Текст]: / Д. В. Бараннік[и др.] // Автоматизированные системы управления и приборы автоматики // 168 - Харьковский национальный университет радиоэлектроники.— 2014.

16. Метод криптокомпрессионных преобразований с ключом [Текст]: / Д. В. Бараннік[и др.] // Сучасна спеціальна техніка // 1 - Міністерство внутрішніх справ України, Державний науково-дослідний інститут МВС України.— 2018 – С. 51 - 57.