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 (ПРОЕКТ)
Пояснювальна записка

_____*БАКАЛАВР*_____
(освітній ступінь)

_____ГЮІК.504300.0036 ПЗ_____
(позначення документа)

Структурно-стеганографічне кодування з плаваючим базисом вбудовування для підвищення безпеки інформаційних ресурсів
(тема)

Виконав: студент IV курсу, групи КІ-14-7

спеціальності (напряму підготовки) _____

_____*6.050102 – Комп'ютерна інженерія*__

_____
(шифр і назва спеціальності, напряму)

_____ Бараннік Д.В.
(підпис) (прізвище, ініціали)

Керівник роботи_____ Литвинова Є.І.
(підпис) (прізвище, ініціали)

Допускається до захисту

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

2018 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра автоматизації проектування обчислювальної техніки

Рівень вищої освіти перший (бакалаврський)

Напрям 6.050102 – Комп'ютерна інженерія
(код і повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2018 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

Студентові Баранніку Дмитру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Структурно-стеганографічне кодування з плаваючим базисом вбудовування для підвищення безпеки інформаційних ресурсів

затверджена наказом по університету від 25.05.2018 р. № 608 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 08 червня 2018 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 структурно-комбінаторного 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 структурно-комбінаторного 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.	Аналіз завдання	01.05.2018	
2.	Огляд літератури за темою роботи	01.05.2018	
3.	Опис методу безпосереднього стеганографічного вбудовування для відеоконтейнера	10.05.2018	
4.	Опис методологічних аспектів вдосконалення технологій безпосереднього стеганографічного вбудовування	15.05.2018	
5.	Розробка методу структурно-комбінаторного стеганографічного кодування	20.05.2018	
6.	Оцінка характеристик ефективності функціонування розробленого методу стеганографічного кодування	20.05.2018	
7.	Розробка програмного забезпечення хмарного сервісу квантового моделювання цифрових схем	30.05.2018	
8.	Оформлення пояснювальної записки	02.06.2018	
9.	Оформлення презентації	06.06.2018	
10.	Представлення роботи до захисту	08.06.2018	

Дата видачі завдання _____ _____2018 р.

Студент _____
(підпис)

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

РЕФЕРАТ

Пояснювальна записка атестаційної роботи бакалавра: містить 79 с. основного тексту, 40 рис., 6 табл., 2 дод., 10 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. Розроблене програмне забезпечення для реалізації запропонованої технології.

ABSTRACT

Bachelor Diploma Thesis contains: 79 pages of the main text, 40 figures, 6 tables, 2 annexes, 10 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 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

ДНК – дезоксирибонуклеїнова кислота

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 значимістю СІР для інформаційної підтримки процесів ухвалення рішень, у тому числі в кризових ситуаціях. З іншого боку підвищуються загрози порушення конфіденційності і 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.

Проте проведений аналіз існуючих методів виявив наступні 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. Тут слід виділити такі аспекти актуальності і значущості стеганографічних методів:

1. 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.

2. Обмеження при використанні криптографічних алгоритмів захисту спеціальних інформаційних ресурсів. Вони мають негативні наслідки і можуть завдати збитки політичному і економічному іміджу держави.

3. Формування умов для розвитку стеганографічних підходів забезпечення безпеки спеціальних інформаційних ресурсів обумовлюються наступними позиціями:

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

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

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

г) 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 наступні 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.

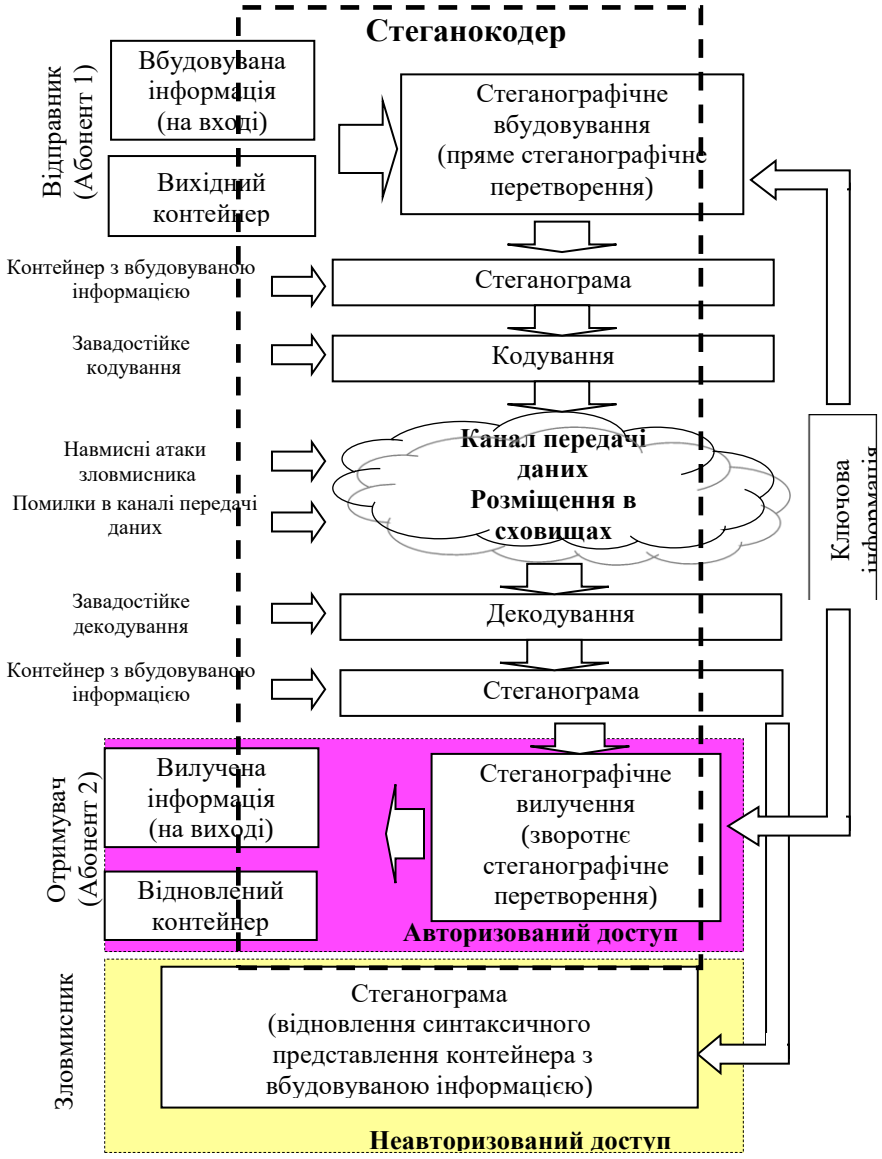

Рисунок. 1.1 – Функціональна схема реалізації прихованої передачі даних на основі стеганографічного підходу

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.

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 $w_{отн}$ стеганографічної системи. Величина $w_{отн}$ відносної стеганографічної ємності системи визначається на основі наступної формули:

$$w_{отн} = \frac{w_{встр}}{W_{исх}} . \qquad (2.2)$$

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

$$w_{отн} = \frac{w_{встр}}{W_{исх}} \cdot 100\% . \qquad (2.3)$$

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 убудовуваної 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 $P_{из}$ безпомилкового вилучення вбудованих даних авторизованим користувачем. Ймовірність $P_{из}$ визначається на основі наступного виразу:

$$P_{из} = \frac{w_{из}}{w_{встр}}, \quad (2.5)$$

де $w_{встр}$ - об'єм вбудовуваної інформації, біт;

$w_{из}$ - 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.

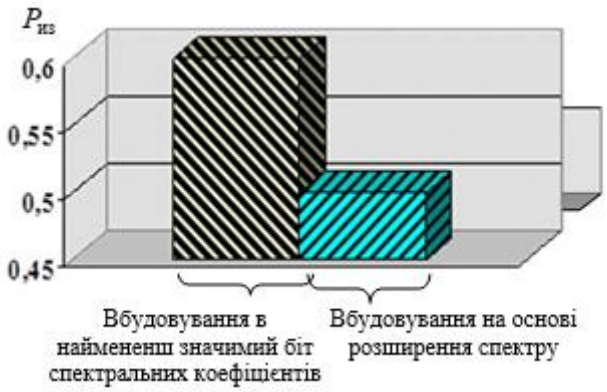

Рисунок 2.1 - Діаграма значень ймовірності $P_{из}$ для методів НЗБ в режимі 2, РС за умов відсутності атак на вбудоване повідомлення

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.

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 $\mathrm{F}\{P_{из},\ w_{отн},\ h\}$ в умовах виконання наступних обмежень:

$$\begin{cases} P_{из} \geq P_{из}^{(тр)}; \\ w_{отн} \geq \mathrm{w}_{отн}^{(тр)}; \\ h \geq h^{(тр)}; \end{cases} \tag{2.8}$$

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

$\mathrm{w}_{отн}^{(тр)}$ - 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 $A_2 = [A]_2$.

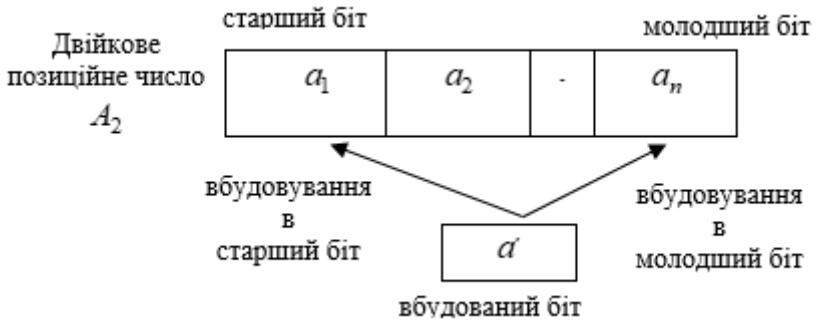

Рисунок 3.1 - Схема вбудовування біта приховуваного повідомлення в елемент поточного представлення зображення-контейнера

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

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.

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).

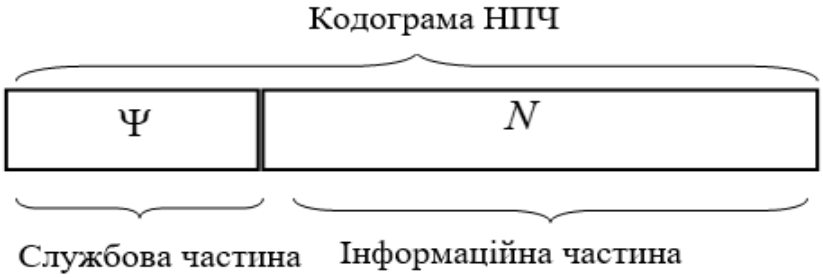

Рисунок 3.2 - Схема кодограми для нерівновагового позиційного числа

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 .

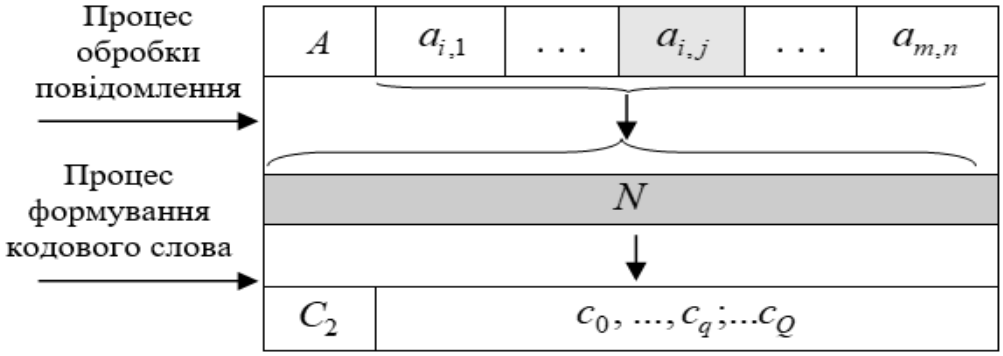

Рисунок 3.3 - Структурна схема побудови кодових конструкцій для нерівновагового позиційного числа А

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).

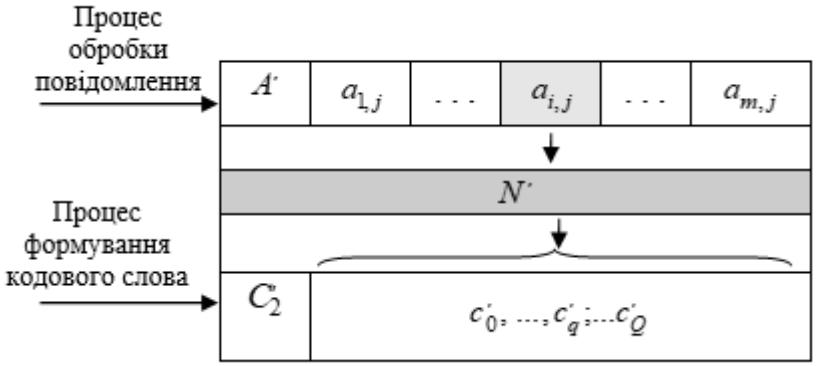

Рисунок 3.4 - Структурна схема побудови кодових конструкцій НП числа A' з вбудованими даними

У вихідне нерівновагове позиційне число A за допомогою оператора φ' вбудовується біт b_ξ приховуваного повідомлення В 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.

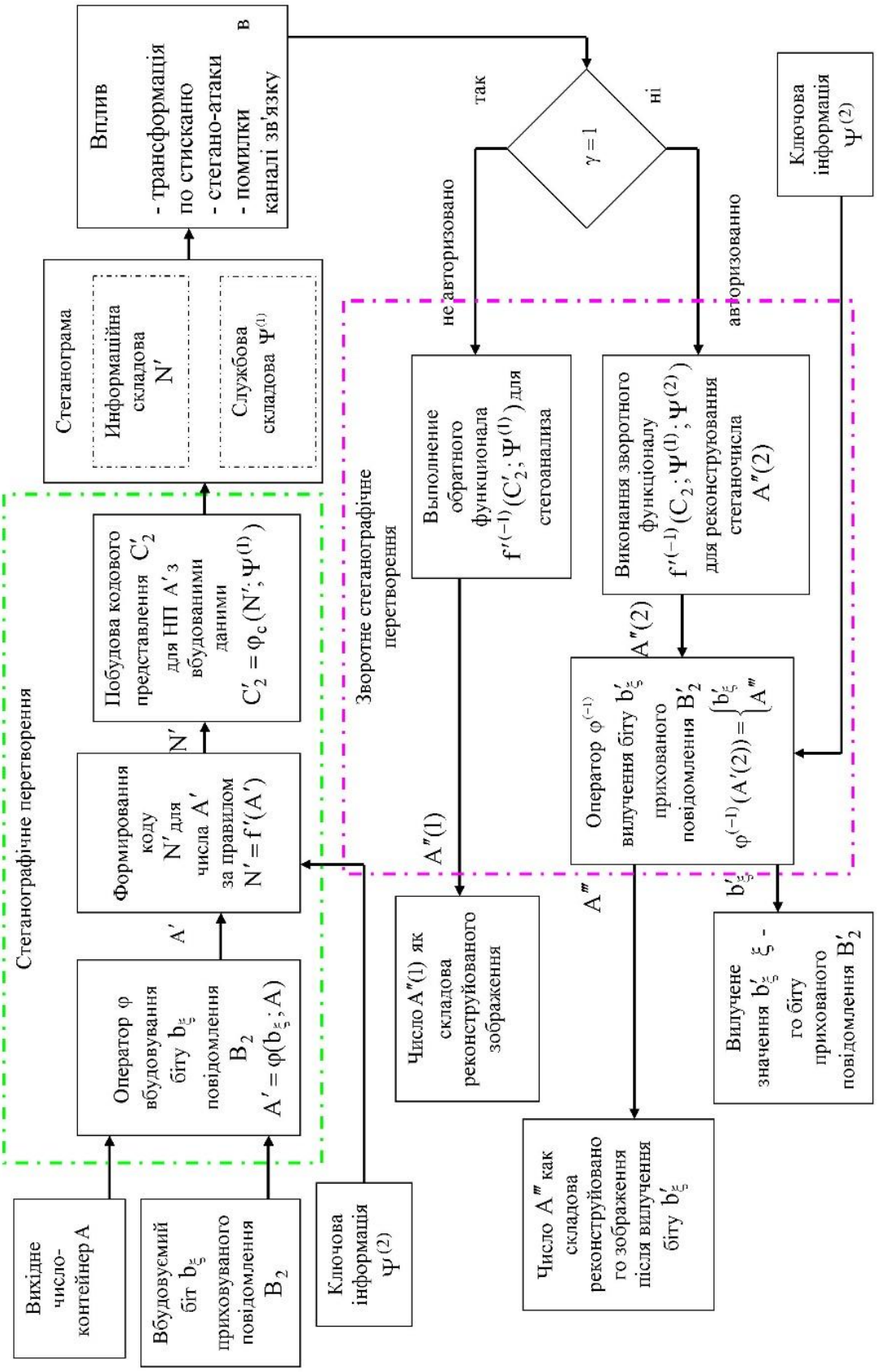

Рисунок 3.5 - Схема стеганографічного перетворення на основі нерівновагового позиційного кодування

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 РОЗРОБКА МЕТОДУ СТРУКТУРНО-КОМБІНАТОРНОГО СТЕГАНОГРАФІЧНОГО КОДУВАННЯ

4.1 Розробка моделі структурно-комбінаторного стеганографічного кодування

Для проектування стеганосистеми пропонується використовувати наявність в зображенні-контейнері структурно-комбінаторних закономірностей, обумовлених наявністю обмежень на динамічний діапазон.

Величина ψ_i динамічного діапазону рядка масиву зображення-контейнера $A = \{a_{i,j}\}$ визначається на основі наступного виразу:

$$\psi_{i,j} = \min(\psi_i;\ \psi_j). \tag{4.1}$$

Схема формування базису динамічних діапазонів для зображення-контейнера A представлена на рис. 4.1.

Для задоволення вимоги обліку обмеження на динамічний діапазон в процесі представлення і кодування пропонується використовувати нерівновагове представлення. Тому пропонується проектувати стеганосистему на основі кодоутворювального функціоналу з врахуванням нерівновагового позиційного базису.

В якості кодоутворювального функціонального перетворення пропонується використовувати кодоутворювальну функцію для нерівновагового позиційного числа. Така функція володіє властивостями для відповідності вимогам відносно процесу приховування даних, а саме:

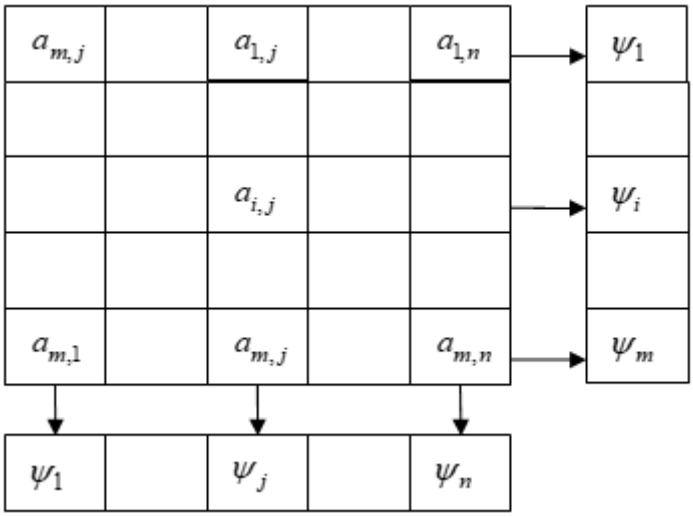

Рисунок 4.1- Схема формування базису динамічних діапазонів для зображення-контейнера А.

1) формування стеганограми C з використанням кодоутворювального функціоналу для нерівновагового позиційного числа здійснюється за інтегральним принципом в два етапи. На першому етапі для вихідного нерівновагового позиційного числа, як результат застосування функціоналу $f(A'_{cu})$ до числа з імплантацією A'_{cu}, формується кодове значення, що містить інформацію про елементи числа A'_{cu}, тобто

$$N = f(A'_{cu}). \tag{4.2}$$

На основі сформованого значення коду N на другому етапі будується результуюче кодове представлення C_2 стеганограми. Це визначається наступним виразом:

$$C_2 = \varphi_c(N). \tag{4.3}$$

Тут φ_c - оператор, який забезпечує побудову двійкового коду C_2 для кодового значення N;

2) зворотнє перетворення виконується за біполярним принципом для

авторизованого (за наявності ключа $\Psi^{(2)}$) і неавторизованого користувача (зловмисника) за стандартних умов.

Перший спосіб відповідає неавторизованим користувачам. Відновлення зображення відбувається за наявності відкритої службової інформації $\Psi^{(1)}$, що являє собою систему нерівновагових позиційних базисів основ числа A'_{ou} до здійснення імплантації.

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 $\Psi^{(2)} \neq \Psi^{(1)}$.

3) стеганограма C, містить відомості про вектор службової інформації $\Psi^{(1)}$, за наявності якого можлива реконструкція елементів стеганографічного зображення $A(1)''$ за відсутності інформації про наявність вбудованого повідомлення. Дана властивість задається наступним виразом:

$$C = \varphi_c(N, \Psi^{(1)}), \qquad A(1)'' = f^{(-1)}(C; \Psi^{(1)}). \tag{4.4}$$

В процесі реалізації функціонального перетворення на основі нерівновагового позиційного кодування область вихідного зображення, що містить сукупність відеопослідовностей, розглядається як множина нерівновагових позиційних чисел $\{A(j)\}$. Тут нерівновагове позиційне число $A(j)$ без імплантації для j -го стовпця масиву відеозображення складається з m елементів, тобто

$$A(j) = \{a_{1,j}; ...; a_{i,j}; ...; a_{m,j}\}. \tag{4.5}$$

На даному етапі структурно-комбінаторна надлишковість ще не скорочується. Усунення надлишковості здійснюється на другому етапі в процесі кодування нерівновагового позиційного числа $A(j)$ без імплантації.

Правило $f(A(j))$ передбачає формування коду-контейнера $N(j)$ для нерівновагового позиційного числа $A(j)$ без імплантованого елементу по формулі:

$$N(j) = f(A(j), V^{(1)}), \tag{4.6}$$

де $V^{(1)}$ - система вагових коефіцієнтів нерівновагового позиційного числа $A(j)$ без імплантації в коді-контейнері, яка визначається за допомогою системи основ $\Psi^{(1)}$.

Фізичний зміст вагового коефіцієнта $V_{i,j}$ можна інтерпретувати як умовну кількість інформації, що міститься в $(m-i)$ елементах НП числа при виконанні умови, коли значення i -го елементу рівне $a_{i,j}$.

На цьому етапі фактично закінчуватиметься процес вбудовування інформації.

Кодограма $C(A(j))$ для коду-контейнера $N(j)$ нерівновагового позиційного числа без імплантації $A(j)$ формується на третьому етапі за допомогою оператора виділення розрядів $\varphi_c(\bullet)$ по формулі:

$$C(A(j) = \varphi_c(N(j), \Psi^{(1)}) = \varphi_c(A(j); \Psi^{(1)}; V),$$

де $\Psi^{(1)}$ - ключова складова, що містить систему основ нерівновагового позиційного числа $A(j)$;

$V^{(1)}$- значення вагових коефіцієнтів елементів нерівновагового позиційного числа $A(j)$.

В цьому випадку отримаємо наступну кодограму:

$$C(A(j)) = \{c_1, \ldots, c_\xi, \ldots, c_{q(j)}\}, \tag{4.7}$$

де $q(j)$ - довжина двійкової кодограми $C(A(j))$;

c_ξ - ξ-й двійковий розряд кодограми $C(A(j))$.

Процес реконструкції елементу $a_{i,j}$ для нерівновагового позиційного числа $A(j)$ без вбудованої інформації на основі коду-контейнера $N(j)$ виконується по формулі

$$a_{i,j} = f^{(-1)}(N(j), V_{i,j}, \psi_{i,j}), \tag{4.8}$$

де $V_{i,j}$ - ваговий коефіцієнт елементу $a_{i,j}$.

На рис. 4.2. графічно відображено етапи формування кодограми $C(A(j))$ для кода-контейнера $N(j)$ нерівновагового позиційного числа $A(j)$ (прямого нерівновагового позиційного перетворення) і його декомпозиції (зворотнього нерівновагового позиційного перетворення).

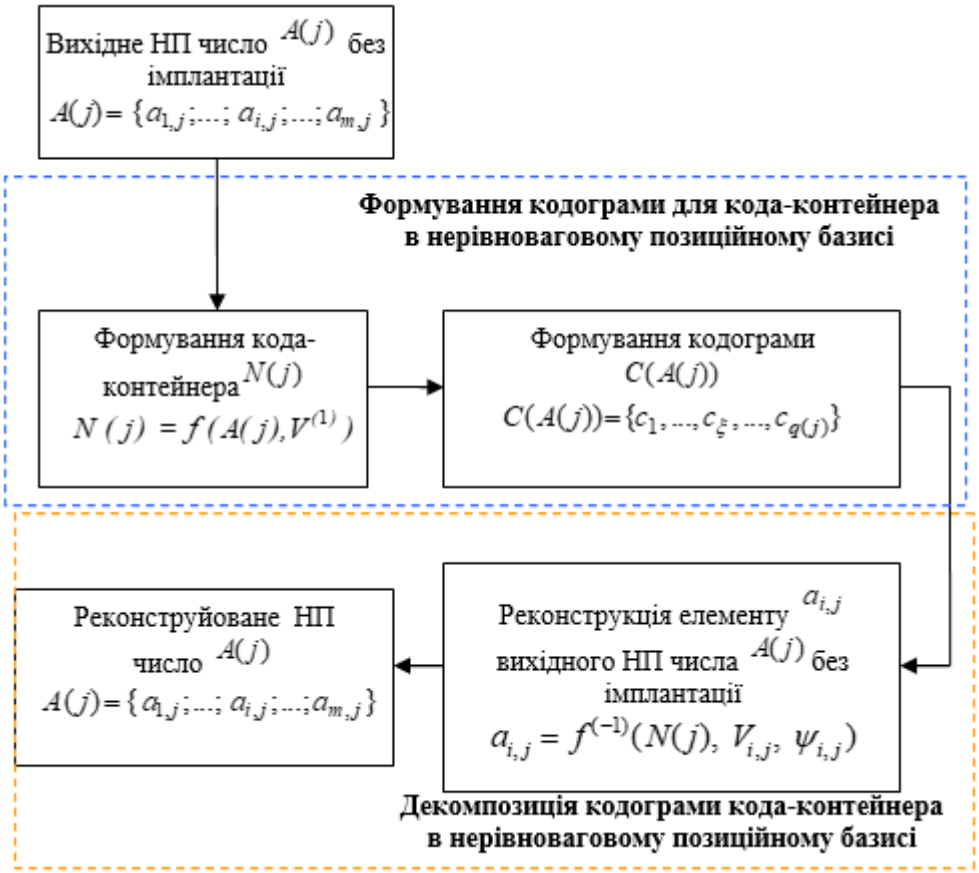

Рисунок 4.2 - Схема стеганографічної системи на основі формування кода-контейнера в нерівновагову позиційному базисі.

Ключова складова $\Psi^{(1)}$ включає інформацію про систему основ $\Psi^{(1)}=\{\psi_{i,j}\}$ нерівновагового позиційного числа без імплантації. Основа $\psi_{i,j}$ визначається як мінімальне значення з двох динамічних діапазонів рядка ψ_i і стовпця ψ_j, на перетині яких вона розташована, тобто $\psi_{i,j}=\min(\psi_i;\psi_j)$. На основі набутих значень основ будується нерівноваговий базис $\Psi^{(1)}=\{\psi_{i,j}\}$ (рис. 4.3).

$\psi_{1,1}$		$\psi_{1,j}$		$\psi_{1,n}$
		$\psi_{i,j}$		
$\psi_{m,1}$		$\psi_{m,j}$		$\psi_{m,n}$

Рисунок 4.3 - Структура нерівновагового базису основ.

Такий підхід при формуванні базису основ для нерівновагового позиційного числа дозволяє виявити структурно-комбінаторні закономірності на динамічний діапазон. Це створює потенціал для встановлення кількості структурно-комбінаторної надлишковості, яку можна буде використовувати для прихованого вбудовування інформації.

Проведемо обґрунтування, що в цих умовах забезпечується можливість приховати вбудовану інформацію в коді-контейнері.

Необхідно оцінити величину структурно-комбінаторної надлишковості, яка потенційно може бути використана для вбудовування інформації в код-контейнер. Для цього порівняємо кількість біт $q(j)_{исх}$, необхідного для двійкового представлення числа $A(j)$ вихідної відеопослідовності з фіксованим динамічним діапазоном і кількість біт $q(j)$ необхідного для представлення кодограми $C(A(j))$.

Значення яскравості елементу просторово-часового представлення зображення-контейнера в системі RGB може набувати значень $a_{i,j} \in [0; 255]$. Іншими словами, для кожного i -го елементу числа $A(j) = \{a_{i,j}\}$ вихідної відеопослідовності величина динамічного діапазону дорівнюватиме 256. Тоді $q(j)_{исх}$ описуватиметься виразом:

$$q(j)_{исх} = m \cdot \log_2 256 = 8 \cdot m \text{ (біт).} \quad (4.9)$$

Визначимо кількість біт $q(j)$, яка необхідна для представлення кодограми $C(A(j))$, отриманої в процесі формування кода-контейнера $N(j)$ нерівновагового позиційного числа $A(j)$. На основі використання властивості нерівновагових позиційних чисел $A(j)$ можна зробити висновок, що для заданого базису основ $\Psi^{(1)}$ максимально можливе значення кода-контейнера $N(j)$ буде обмежено зверху накопиченим добутком $V_{\max}$ основ елементів нерівновагового позиційного числа. Це задається наступним виразом:

$$N(j) \le V_{\max} = f_{осн}(\Psi^{(1)}) + 1. \quad (4.10)$$

Іншими словами, величина $V_{\max}$ визначає кількість різних кодів-контейнерів, які можуть бути сформовані для заданої системи основ $\Psi^{(1)}$.

Звідси, довжина $q(j)$ кодограми інформаційної частини кода-контейнера $N(j)$ визначається на основі наступного виразу:

$$q(j) = |C(A(j))| = [\ell og_2(f_{осн}(\Psi^{(1)}))] + 1 \text{ (біт).} \quad (4.11)$$

Необхідно враховувати, що основа елементів просторово-часового представлення вихідної відеопослідовності приймає значення $\psi_{i,j} \in [1;256]$. Тоді кількість біт $q(j)$, необхідна для двійкового представлення кодограми $C(A(j))$ кода-контейнера $N(j)$ набуде значення:

$$q(j) = C(A(j)) \in [0;\ 8 \cdot m] \text{ (біт).} \qquad (4.12)$$

З врахуванням чого кількість $R(j)$ структурно-комбінаторної надлишковості обчислюється як різниця між кількістю біт $q(j)$ для двійкового представлення кодограми $C(A(j))$ і кількістю біт $q(j)_{исх}$, необхідних для двійкового представлення числа $A(j)$ вихідної відеопослідовності і описується виразом

$$R(j) = q(j)_{исх} - q(j). \qquad (4.13)$$

Тут $R(j)$ - кількість структурно-комбінаторної надлишковості, що виникає в процесі функціонального перетворення на основі формування кода-контейнера нерівновагового позиційного числа $A(j)$. Іншими словами, це надлишковість, що виникає в процесі формування кода-контейнера $N(j)$ для нерівновагового позиційного числа $A(j)$ в результаті формування нерівновагового базису основ відносно кодового представлення вихідної відеопослідовності.

4.2 Розробка концепції стеганографічного кодування нерівновагового числа з імплантованим елементом

Для реалізації виявленої потенційної можливості відносно вбудовування інформації на основі структурно-комбінаторних характеристик пропонується підхід у вигляді формування стеганокоду для числа з імплантованими даними в нерівноваговому позиційному базисі.

Імплантацію в число $A(j)$ пропонується проводити поелементно, тобто один елемент b_ξ на позицію γ-го розряду числа $A(j)$. Тут b_ξ - ξ-й елемент вбудовуваної послідовності $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0;\ 255]$, $\xi = \overline{1, \nu}$. В цьому випадку імплантація визначається по наступній формулі :

$$A(j)' = A(j) \cup b_{\xi}, \text{ у разі коли } b_{\xi} = a'_{\gamma,j} \quad . \tag{4.14}$$

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

$$A(j)' = \{ a_{1,\mathrm{j}};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j} \}, \tag{4.15}$$

де $A(j)'$ - число з імплантованим елементом $a'_{\gamma,j}$ в γ -й розряд числа;

$(m+1)$ - кількість елементів в числі з імплантацією.

На наступному етапі число $A(j)'$ з імплантованим елементом кодується. На цьому етапі проводиться вбудовування приховуваної інформації в код-контейнер. У зв'язку з чим, сформулюємо наступні визначення.

Визначення 4.1. Процес одночасного вбудовування інформації і побудови кода-контейнера, тобто коли вбудовування інформації здійснюється в процесі формування кода-контейнера, називається стеганографічним кодуванням.

Визначення 4.2. Значення кода-контейнера, що містить приховувану інформацію, називається стеганокодом.

Визначення 4.3. Формування стеганокоду на основі кодування нерівновагового позиційного числа з імплантованим елементом приховуваного повідомлення називається структурно-комбінаторним стеганографічним кодуванням в нерівноваговому позиційному базисі.

Значення стеганокода $N(j)'$ для нерівновагового позиційного числа з імплантацією визначається по наступній формулі:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}) \tag{4.16}$$

Тут $V^{(2)}$ - ваговий коефіцієнт імплантованого елементу $a'_{\gamma,j}$.

В разі такого вбудовування фрагмент вихідної відеопослідовності розглядається, як позиційне число $A(j)' = \{ a_{1,\mathrm{j}};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j} \}$ з

імплантованим елементом $a'_{\gamma,j}$, $i=\overline{1,m+1}$. Для числа $A(j)'$ кодове представлення $C(A(j)')$ його стеганокоду $N(j)'$ в нерівноваговому позиційному базисі формується в два етапи (рисунок 3.4).

Перший етап включає обчислення значення стеганокода $N(j)'$, як зваженого сумування величин $a_{i,j}V'_{i,j}$ і величини $a'_{\gamma,j}V'_{\gamma,j}$. Кодограма $C(A(j)')$ стеганокода формується на другому етапі для значення величини $N(j)'$:

$$C(A(j))'=\{c_1,...,c_\tau,...,c_{q(j)'}\}, \tag{4.17}$$

де $q(j)'$ - довжина кодограми $C(A(j)')$.

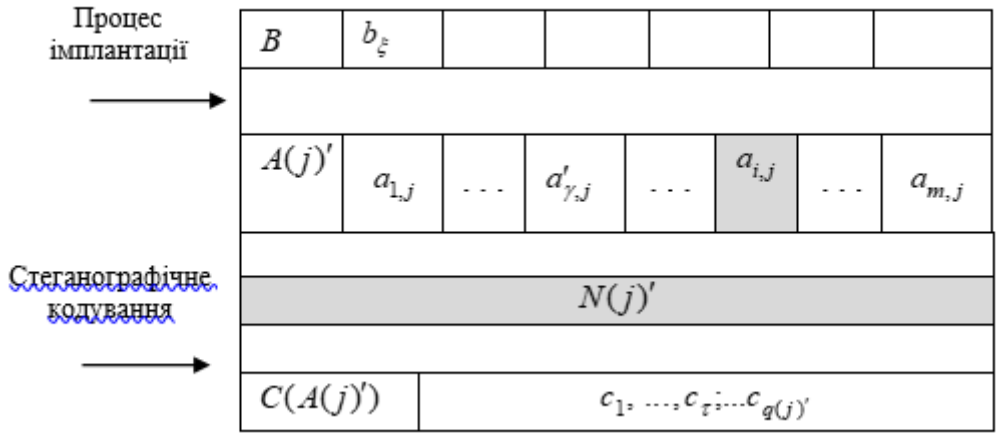

Рисунок 4.4 - Структурна схема побудови кодограми стеганокоду для числа $A'(j)$ з імплантацією

В результаті стеганографічного кодування формуються кодові комбінації, що складаються з двох частин: службової $\Psi^{(1)}$ та інформаційної $N(j)'$ (значення стеганокоду). У зв'язку з чим сформулюємо наступне визначення:

Визначення 4.4. Кодову комбінацію, яка містить службову частину $\Psi^{(1)}$ (система основ) і інформаційну частину (кодове представлення стеганокоду $N(j)'$) називатимемо стеганограмою.

Таким чином, вбудовування елементу в нерівновагове позиційне число здійснюється внаслідок кодування в два етапи. На першому етапі для НПЧ з імплантацією формується стеганокод. Другий етап передбачає формування кодограми для значення стеганокоду. В результаті стеганографічного перетворення формується стеганограма, що містить службову і інформаційну частини.

4.3 Розробка стеганографічної системи з маскуванням структурної стеганографічної надлишковості

Розглянемо як впливає помилкове значення $N(j)''$ кода-контейнера, зчитане з інформаційної частини кодограми в умовах, коли:

- з одного боку в реальності передається стеганокод $N(j)'$;

- з іншого боку неавторизований користувач зчитуватиме значення кода-контейнера $N(j)$.

В цьому випадку замість того щоб відібрати $q(j)'$ біт, неавторизований користувач вибирає $q(j)$ біт.

Розглянемо процес реконструкції елементів вихідної відеопослідовності, представлених як нерівновагові позиційні числа в умовах використання помилкового значення кода-контейнера $N(j)''$. Іншими словами проведемо оцінку впливу невідповідності довжини стеганокоду і кода-контейнера на процес відновлення елементів вихідної відеопослідовності. Розглянемо реконструкцію i-го елементу j-ої відеопослідовності. Для цього використовуємо вираз:

$$a''_{i,j} = f^{(-1)}\left(N(j)''_i, V_{i,j}, \psi_{i.j}\right), \tag{4.18}$$

де $a''_{i,j}$ - i-й елемент реконструйованої відеопослідовності;

$N(j)''_i$ - залишкове значення коду нерівновагового позиційного числа для

декодування чергового i-го елементу.

З аналізу цього виразу в умовах, коли

$$N(j)'' > N(j)', \tag{4.19}$$

слідує що, як мінімум починаючи з деякої β-ої позиції, елементи відеопослідовності обнулятимуться, тобто

$$a''_{i,j} = 0, \quad \text{для} \quad i = \overline{\beta; m+1}. \tag{4.20}$$

Таким чином, помилково встановлена зловмисником довжина інформаційної частини $N(j)''_i$ приводитиме до появи спотворень в процесі відновлення відеозображення. Дані візуальні спотворення можуть служити додатковим джерелом для стегоаналізу.

Тому для усунення впливу стеганографічної надлишковості на можливість проведення атаки зловмисником, у тому числі встановлення факту наявності вбудованої інформації, необхідно розробити підхід для усунення стеганографічної надлишковості. Спочатку надамо наступне визначення.

Визначення 4.5. Процес локалізації кількості надлишковості, що виникає в процесі стеганографічного кодування будемо назвати структурним стеганографічним маскуванням або маскуванням структурної стеганографічної надлишковості.

Локалізацію структурної стеганографічної надлишковості в процесі формування стеганокоду в нерівноваговому базисі пропонується здійснювати на основі корекції довжини кодограми $C(A(j)')$ стеганокоду $N(j)'$. Процес корекції передбачає приведення довжини кодограми стеганокоду $q(j)'$ до значення довжини $q(j)$. У фізичному плані, реалізація корекції кодограми полягає у відкиданні $(\log_2 \psi'_{\gamma,j})$ найменш значимих біт кодограми $C(A(j)')$, тобто

$$C'''_j = [N(j)''']_2 = [N(j)' / \psi'_{\gamma,j}]_2, \tag{4.21}$$

де $N(j)'''$ - значення стеганокоду, скоректоване в процесі маскування структурної стеганографічної надлишковості;

$[N(j)''']_2$ - двійкове значення скоректованого стеганокоду $N(j)'''$;

C_j''' - кодограма кодового представлення скоректованого стеганокоду $N(j)'''$.

Ступінь локалізації значення стеганокоду, а значить і рівень його спотворень, залежатиме від значення основ $\psi'_{\gamma,j}$ вбудовуваного елементу. Тоді для забезпечення появи мінімального значення $R(j)_{стег}$ в процесі стеганографічного кодування повинна виконуватися умова:

$$(\log_2 \psi'_{\gamma,j}) \to \min . \qquad (4.22)$$

Тому для зменшення рівня спотворень стеганокоду пропонується вбудовувати елементи в двійковому представленні, тобто $b_\xi \in [0;1]$. В цьому випадку основа вбудованого елементу буде рівна $\psi'_{\gamma,j} = 2$.

Визначимо довжину $q(j)'$ кодограми стеганокоду N(j)′ числа $A(j)'$ з імплантацією двійкового елементу. Враховуючи, що імплантований елемент $a'_{\gamma,j}$ має основу $\psi'_{\gamma,j} = 2$, то величина $q(j)'$ визначатиметься по формулі:

$$q(j)' = [\ell og_2 \psi'_{\gamma,j} + \ell og_2 (f_{осн}(\Psi^{(1)}))] + 1 \text{ (біт).} \qquad (4.23)$$

Можна зробити висновок, що імплантація біта в число $A(j)$ збільшує довжину кодового представлення стеганокоду відносно кода-контейнера на один біт. Кількість $R(j)_{стег}$ структурної надлишковості буде дорівнювати:

$$R(j)'_{стег} = q(j)' - q(j) = 1 \text{ (біт).} \qquad (4.24)$$

Отже, вбудовування двійкового елементу дозволяє мінімізувати ступінь невідповідності між значеннями стеганокоду і кода – контейнера. В цьому випадку правило локалізації матиме вигляд:

$$C_j''' = [N(j)''']_2 = [N(j)'/2]_2 . \quad (4.25)$$

Такий варіант локалізації стеганографічної надлишковості полягає у використанні властивостей стійкості структурних характеристик і структурно-комбінаторної надлишковості кодів відносно обробки спотворених значень кодів нерівновагового позиційного числа. Після локалізації стеганографічної надлишковості довжина $q(j)''$ кодограми скоректованого стеганокоду $N(j)'''$ обчислюватиметься за допомогою наступної формули:

$$q(j)'' = [(\ell og_2 \psi'_{\gamma,j} + \ell og_2 (f_{осн}(\Psi^{(1)})))/2] + 1 = q(j) . \quad (4.26)$$

Як показує аналіз виразу (4.25) спотворення в значенні стеганокоду все одно вноситимуться. Причому найбільшим спотворенням піддаватимуться молодші елементи нерівновагового позиційного числа. Тому для підвищення стійкості вбудованих даних пропонується розміщувати один біт приховуваної інформації на позицію старшого елементу нерівновагового позиційного числа.

Внаслідок такого вбудовування число $A(j)'$ прийме наступний вигляд:

$$A(j)' = \{a'_{1,j}; a_{2,j}; ...; a_{i,j}; ...; a_{m+1,j}\}, \quad (4.27)$$

де $A(j)'$ - число з імплантованим бітом $a'_{1,j}$ на позиції старшого елементу;

$a'_{1,j}$ - імплантований біт на позиції старшого елементу числа $A(j)'$, рівний

$$a'_{1,j} = b_\xi, \quad a'_{1,j} \in [0;1], \quad (4.28)$$

де b_ξ - ξ-й елемент вбудовуваної послідовності $B = \{b_1; ...; b_\xi; ...; b_\nu\}$; $b_\xi \in [0;1]$, $\xi = \overline{1,\nu}$;

$(m+1)$ - кількість елементів в числі $A(j)'$ з імплантацією.

В цьому випадку вага вбудовуваного елементу $V'_{\gamma,j}$ в нерівноваговому позиційному числі буде найбільшою, тобто

$$V'_{\gamma,j} = V'_{1,j} = \max_{1 \le i \le m+1} .\{V'_{i,j}\} . \quad (4.29)$$

Отже, вбудовуваний елемент буде стійкіший до перетворень із стеганокодом. В той же час вбудовування приховуваного елементу на старшу позицію в числі забезпечує виключення впливу його основи на реконструкцію елементів вихідної відеопослідовності.

На рис. 4.5 схематично відображено утворення мінімальної структурно-комбінаторної стеганографічної надлишковості для кодограми стеганокоду відносно кодограми кода-контейнера при вбудовуванні двійкового елементу на позицію старшого елементу нерівновагового позиційного числа.

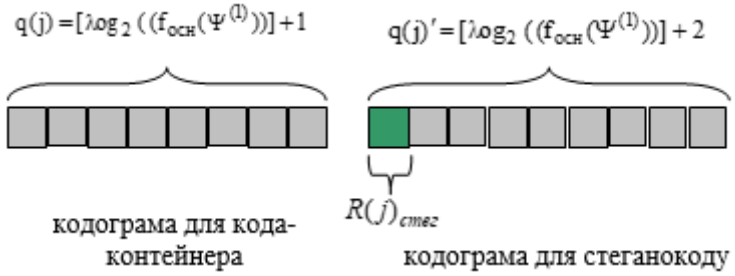

Рисунок 4.5 - Кодограма кода-контейнера і стеганокоду

Розглянемо етапи функціонування стеганографічної системи з маскування стеганографічної надлишковості (рис. 4.6). Зазначена система дозволяє вбудувати біт приховуваного повідомлення на старшу позицію нерівновагового позиційного числа в процесі стеганографічного кодування. Отримана в результаті такого кодування стеганограма складається із службової та інформаційної частин. Реалізація вилучення вбудованих даних відбувається за біполярним принципом: для авторизованого і неавторизованого користувача.

Стеганографічна система містить наступні базові складові:

1. Стеганографічне кодування з маскуванням структурної стеганографічної надлишковості.

2. Структурно-комбінаторне демаскувальне декодування.

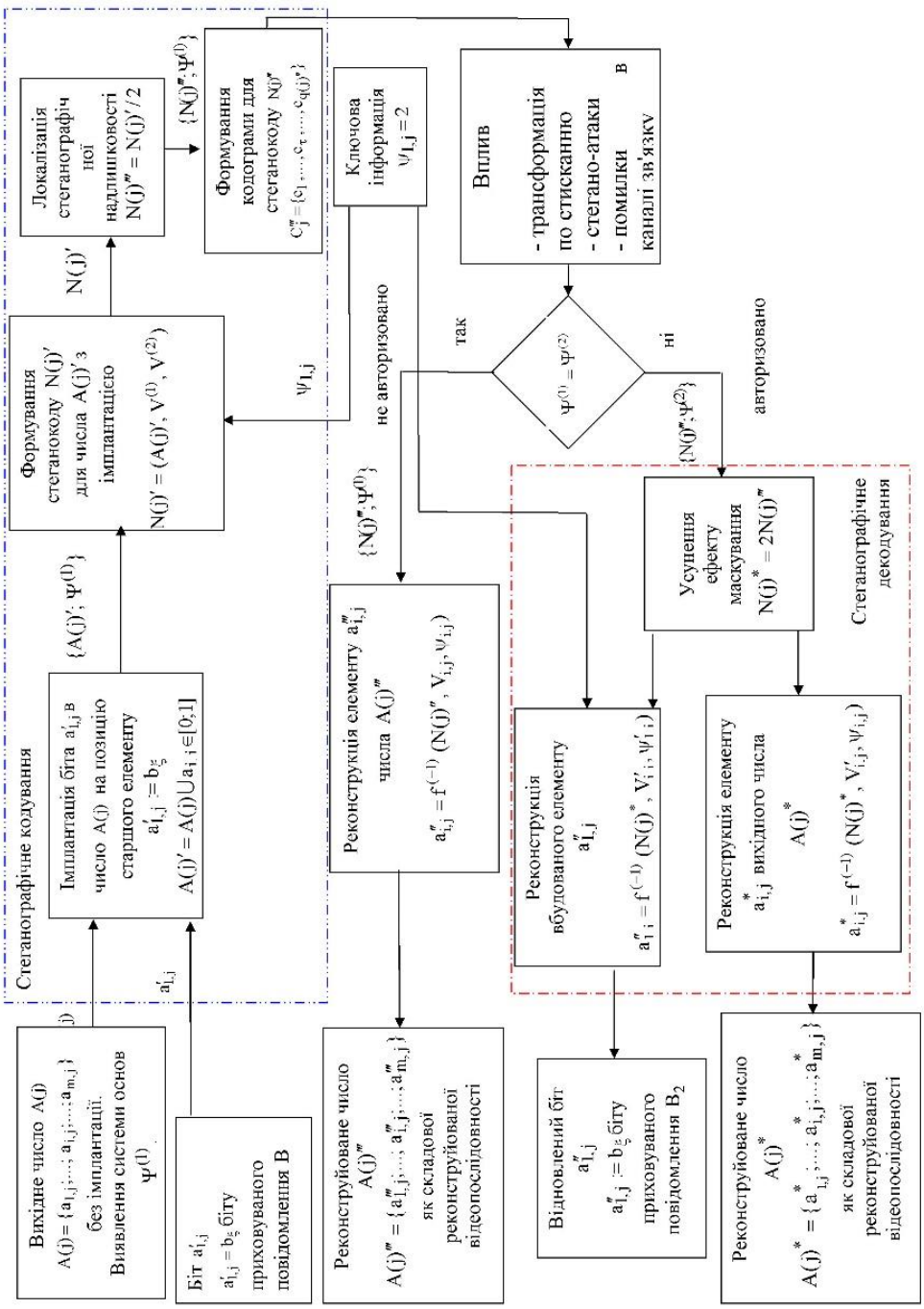

Рисунок 4.6 - Структурна схема стеганографічної системи на основі імплантації приховуваного двійкового елементу на старшу позицію НПЧ з подальшим кодуванням і маскуванням

Розглянемо процес стеганографічного кодування. Даний етап передбачає наступні дії:

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

$$A(j)' = A(j) \cup b_\xi, \text{ для } b_\xi = a'_{1,j} \in [0,\ 1]. \tag{4.30}$$

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

$$A(j)' = \{ a'_{1,j};...;a_{i,j};...;a_{m+1,j} \}, \tag{4.31}$$

де $A(j)'$ - число з імплантованим на старшу позицію елементом $a'_{1,j}$.

2. Формування стеганокоду $N(j)'$ для числа $A(j)'$ з імплантованим елементом $a'_{1,j}$. Враховуючи механізм локалізації кількості структурної стеганографічної надлишковості, вираз для формування стеганокоду $N(j)'$ матиме вигляд:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}). \tag{4.32}$$

3. Маскування структурної стеганографічної надлишковості. Здійснення такого маскування відбувається шляхом корекції стеганокоду $N'(j)$, а саме зменшенням довжини його двійкового представлення на один біт. Для отримання значення скоректованого стеганокоду $N(j)''$ використовується наступний вираз:

$$N(j)'' = N(j)' / 2. \tag{4.33}$$

На рис. 4.7 схематично відображені етапи стеганографічного кодування.

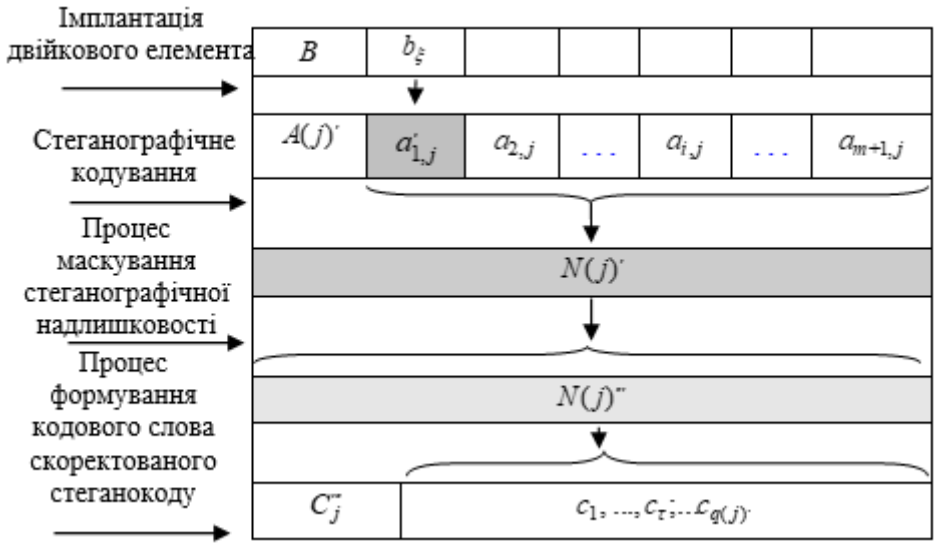

Рис 4.7 - Структурна схема побудови кодограми скоректованого стеганокоду для числа $A'(j)$ з імплантацією

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

$$C''_j = \{c_1, ..., c_\tau, ..., c_{q(j)''}\}, \tag{4.34}$$

де $q(j)''$ - довжина кодограми C''_j рівна $q(j)'' = [(\ell og_2 \psi'_{\gamma,j} + \ell og_2\ (f_{осн}(\Psi^{(1)})))/2] + 1$.

Тепер необхідно розглянути другу базову складову розробленої стеганографічної системи - стеганографічне декодування.

4.4 Розробка структурно-комбінаторного демаскуючого декодування

Розглянемо процес вилучення даних, що містяться в стеганограмі. Для цього введемо наступне визначення.

Визначення. Процес вилучення приховуваної інформації, здійснюваний одночасно з процесом реконструкції кода-контейнера, називається

стеганографічним декодуванням.

Визначення 4.6. Процес одночасного вилучення приховуваної інформації і відновлення нерівновагового позиційного числа на основі реконструкції стеганокоду називається структурно-комбінаторним стеганографічним декодуванням в нерівноваговому позиційному базисі.

Процес стеганографічного декодування в даному випадку здійснюється за біполярним принципом для авторизованого користувача і зловмисника (неавторизований користувач).

В разі неавторизованого доступу, коли у зловмисника немає інформації про позицію стеганокоду в стислому представленні зображення і позиції вбудованого елементу, процес декодування здійснюється на основі наступних етапів:

1. Вилучення з кодограми C_j''' скоректованого стеганокоду $N(j)'''$ за допомогою системи основ $\Psi^{(1)}$.

2. Відновлення елементів вихідної відеопослідовності за формулою:

$$a_{i,j}''' = f^{(-1)}(N(j)''', V_{i,j}, \psi_{i.j}), \tag{4.35}$$

де $a_{i,j}'''$ - i-й елемент реконструйованого числа $A(j)'''$, як складової реконструйованої j-ї відеопослідовності, при неавторизованому доступі.

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

Навпаки, коли проводиться стеганографічне декодування авторизованим користувачем, то йому доступна наступна інформація:

1) позиція стеганокоду в стисненому представленні зображення;

2) позиція вбудованого елементу $a'_{1,j}$;

3) основа вбудованого елементу $a'_{1,j}$.

В цьому випадку стеганографічне декодування буде містити наступні

етапи:

1. Вилучення з кодограми C_j''' скорегованого стеганокоду $N(j)'''$. Таке вилучення здійснюється на основі системи основ $\Psi^{(1)}$, яка міститься в службовій частині стеганограми.

2. Проведення демаскування стеганокоду (усунення ефекту маскування). Для цього введемо наступне визначення.

Визначення 4.7. Стеганографічне декодування з врахуванням демаскованої структурної стеганографічної надлишковості називатимемо демаскуючим стеганографічним декодуванням.

Для цього до двійкового представлення стеганокоду $N(j)''$, вилученого з кодограми C_j''' добавляється один біт, що дорівнює нулю. Значення відновленого стеганокоду $N(j)^*$ визначається за формулою:

$$N(j)^* = N(j)''' * 2. \tag{4.36}$$

3. Відновлення вбудованого елементу $a'_{1,j}$. Даний етап реалізується на основі інформації про позицію стеганокоду в стисненому зображенні, позицію вбудованого елементу і його основи $\psi'_{1,j} = 2$. Для цього використовується наступна формула:

$$a''_{1,j} = f^{(-1)}(N(j)^*, V_{1,j}, \psi'_{1,j}). \tag{4.37}$$

Тут $a''_{1,j}$ - значення вилученого біта вбудованої інформації $b_\xi := a''_{i,j}$.

4. Відновлення інших елементів $a^*_{i,j}$ вихідної відеопослідовності проводиться на основі використання системи основ $\Psi_j^{(1)}$. При цьому застосовується вираз:

$$a^*_{i,j} = [N(j)^* / V'_{i,j}] - [N(j)^* / (\psi_{i,j} V'_{i,j})] \psi_{i,j}, \tag{4.38}$$

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

Розглянемо приклад використання розробленого стеганографічного методу для вбудовування приховуваної інформації. Як вихідні зображення використовуємо наступні (додаток А):

1) зображення «Знімок аеропорту»;

2) зображення «Фотознімок».

Експеримент проводиться в наступних умовах:

1) формуються нерівновагові позиційні числа довжиною $m = 4$;

2) імплантація одного біта інформації $b_{\xi} = 1$ здійснюється на старшу позицію кожного нерівновагового позиційного числа.

Результати обробки зображень «Знімок аеропорту» і «Фотознімок» для неавторизованого користувача представлені відповідно на рис. 4.8 і рис. 4.9.

Рисунок 4.8 - Зображення «Знімок аеропорту», декодоване зловмисником

Рисунок 4.9- Зображення «Фотознімок», декодоване неавторизованим користувачем

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

1. Зображення «Знімок аеропорту» і «Фотознімок» містять незначні візуальні спотворення, а саме: розмиття країв, мозаїчний ефект

2. Значення пікового відношення сигнал-шум відносно вихідного зображення-контейнера складає: для зображення «Знімок аеропорту»- 37,94 дБ, для зображення «Фотознімок»- 33,978 дБ.

Спотворення, які з'явилися в процесі декодування, пояснюються впливом локалізації структурної стеганографічної надлишковості. Неавторизований користувач при декодуванні використовує скоректоване значення стеганокоду $N(j)''$.

Відновлення вихідних значень зображення-контейнера відбувається з помилками.

Реалізація демаскуючого стеганографічного декодування для авторизованого користувача розглядається на прикладі реконструкції зображень «Знімок аеропорту» і «Фотознімок» представлених відповідно на рис. 4.10 і рис. 4.11.

З аналізу зображень, отриманих в процесі стеганографічного декодування з демаскуванням (авторизований доступ) можна зробити наступні висновки:

1. Вся вбудована інформація вилучається без помилок.

2. Реконструйовані зображення мають незначні візуальні спотвореня, які викликані корекцією довжин при стеганорафічному декодуванні.

Корекції у вигляді помилково вилучених елементів розташовані рівномірно, по всьому зображенню незалежно від насиченості зображення.

3. Пікове відношення сигнал-шум відносно зображення-контейнера для стеганографічного декодованого зображення «Знімок аеропорту» складає 61,489 дБ, а для зображення «Лена» 61,399 дБ. Звідси, спостерігається збільшення значення пікового відношення сигнал шум відносно зображень «Знімок аеропорту» і «Фотознімок», декодованих неавторизованим

користувачем, відповідно на 24 дБ і 32 дБ.

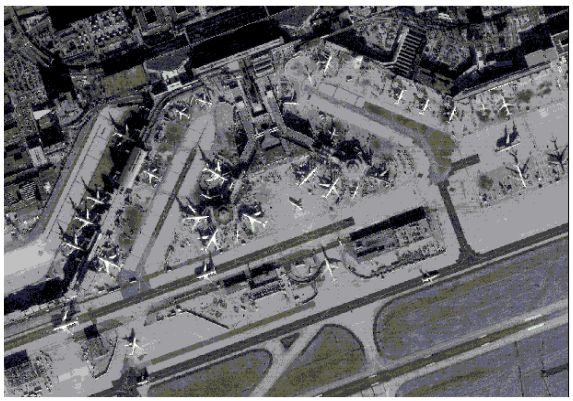

Рисунок 4.10 - Зображення «Знімок аеропорту» отримане в результаті стеганографічного декодування для авторизованого користувача

Рис 4.11 - Зображення «Фотознімок» - отримане в результаті стеганографічного декодування для авторизованого користувача

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

1. Відновлення вбудованої інформації при стеганографічному декодуванні складає 100%.

2. Реконструйовані зображення при неавторизованому доступі містять

незначну кількість візуальних корекцій.

3. З'являється можливість використання зображень, вилучених при демаскувальному стеганографічному декодуванні, в якості корисної інформації.

4. Для насичених зображень оцінка пікового відношення сигнал-шум дає кращі показники порівняно з менш насиченими зображеннями, як при авторизованому доступі, так і для неавторизованого користувача.

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 типізований об'єктно-орієнтована мова програмування. Програми на Java транслюються в байт-код Java, який виконується віртуальною машиною Java (JVM) - програмою, обробній байтовий код і передавальної 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 типізований мова програмування, що працює поверх JVM і розробляється компанією JetBrains. Автори ставили за мету створити мову більш лаконічний і типобезпечний, ніж Java, і більш простий, ніж Scala. Наслідком спрощення в порівнянні зі Scala стали також більш швидка компіляція і краща підтримка мови в IDE.

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

Для реалізації прямого прямого стенаграфічного кодування була написана 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.

```kotlin
@JvmStatic
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.N /= TWO
}
```

Kotlin

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 відкиданні останнього біту коду шляхом ділення його значення на два.

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 написана функція OpcReverceWithMessageAt (рис. 5.2).

```kotlin
@JvmStatic
fun OpcReverceWithMessageAt(dataOrigin: Matrix<Short>, DataOpc: DataOpc, message_position: Int): Boolean {
    DataOpc.N *= TWO
    var copy = BigInteger.ONE
    var b: BigInteger
    var message = false
    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
}
```

Kotlin

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.

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 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 старшого елементу нерівновагового позиційного числа $A(j)$ довжиною m. Множина нерівновагових позиційних чисел $\{A(j)\}$ довжиною m формується окремо для кожної кольорової складової зображення-контейнера.

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. 6.1.

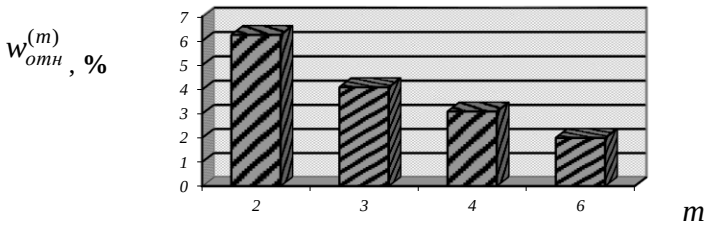

Рисунок 6.1 - Залежність значення $w_{отн}^{(m)}$ відносної стеганографічної ємності стеганографічного алгоритму від довжини m НПЧ

З аналізу рис. 6.1 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).

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:

1) 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 %;

2) 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»	«Фотозні мок»	«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

6.2 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 $\gamma = 1$; основа вбудованого елементу $\psi'_\gamma = 2$.

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

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

2) імплантація одного біта інформації здійснюється на старшу позицію $\gamma = 1$ кожного нерівновагового позиційного числа;

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

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

1) сильно насичене зображення «Знімок аеропорту»;

2) середньо насичене зображення «Фотознімок»;

3) 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. 6.2)

Рисунок 6.2 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 2$

- середньо насичене декодоване зображення «Фотознімок» (рис. 6.3);
- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.4).

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

Рисунок 6.4 - 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. 6.5);
- середньо насичене декодоване зображення «Фотознімок» (рис. 6.6);
- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.7).

Рисунок 6.5 - 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 6.6 - 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. 6.8);
- середньо насичене декодоване зображення «Фотознімок» (рис. 6.9);
- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.10).

Рисунок 6.7 - Зображення «Літак на фоні неба», декодоване неавторизованим користувачем при довжині НПЧ $m = 3$

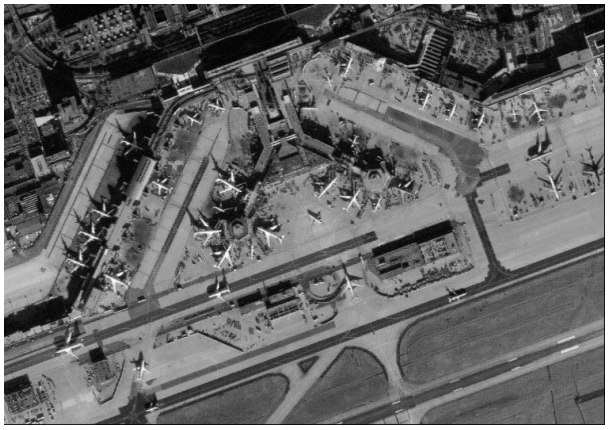

Рисунок 6.8 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 4$

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

Рисунок 6.9 - Зображення «Фотознімок», декодоване неавторизованим користувачем при довжині НПЧ $m = 4$

Рисунок 6.10 - 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. 6.11)

- середньо насичене декодоване зображення «Фотознімок» (рис. 6.12);

- слабо насичене декодоване зображення «Літак на фоні неба» (рис. 6.13).

Рисунок 6.11 - Зображення «Знімок аеропорту», декодоване неавторизованим користувачем при довжині НПЧ $m = 6$

Рисунок 6.12 - Зображення «Фотознімок», декодоване неавторизованим користувачем при довжині НПЧ $m = 6$

Рисунок 6.13 - 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. 6.14 представлені узагальнені результати за оцінкою значення пікового відношення сигнал-шум для декодованих зображень при неавторизованому доступі.

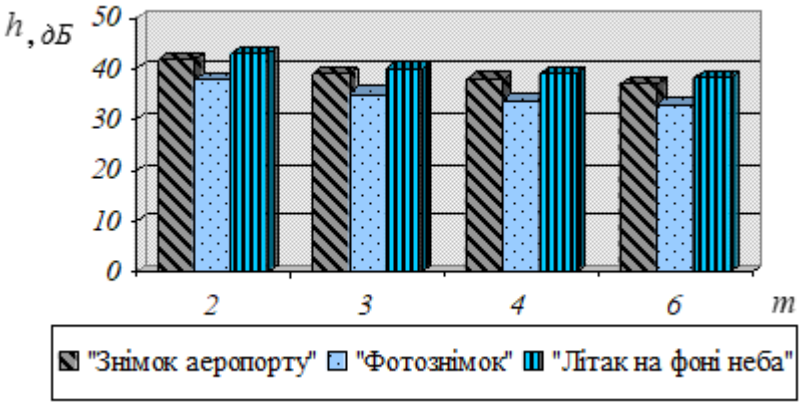

Рисунок 6.14 - Значення ПВСШ h для декодованих зображень при різних значеннях довжини m сформованих НПЧ

З аналізу рис. 6.14 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.

6.3 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. Для розробленого методу, вилучення біта приховуваного повідомлення здійснюється за наявності наступної інформації (авторизований доступ):

- позиція стеганокоду в ефективному синтаксичному представленні зображення;
- позиція $\gamma = 1$ 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 стеганокоду $N'''(j)$ здійснюється шляхом приведення його довжини до значення довжини вихідного стеганокоду $N^{*}(j)$.

На рис. 6.15 представлена порівняльна діаграма значень ймовірності $P_{\text{из}}$ безпомилкового вилучення вбудованих даних для методів найменш значущого біта, розширення спектру і розробленого методу в умовах відсутності атак на вбудоване повідомлення.

З аналізу рисунка 6.15 можна зробити наступні висновки:

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

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

вбудоване повідомлення складає 40%;

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

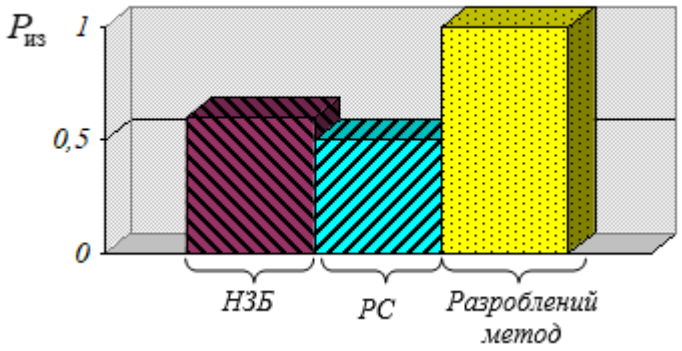

Рисунок 6.15 - Діаграма значень ймовірності $P_{из}$ для методів НЗБ, РС і розробленого методу в умовах відсутності атак на вбудоване повідомлення

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

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

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

6.4 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.

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:

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

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

3) імплантація одного біта інформації здійснюється на старшу позицію $\gamma = 1$ кожного нерівновагового позиційного числа, тобто:

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

4) 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:

1) 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;

2) 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 $m = 2$;

3) 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:

1) 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;

2) 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 $m = 2$;

2) 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 $\boldsymbol{w}_{\text{вост}}$ 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

2) 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 $m = 2$;

3) 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:

1) 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

2) 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 $m = 2$;

3) 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. 6.16 представлена діаграма відсоткового значення кількості безпомилково вилучених бітів для методів НЗБ, РС і розробленого методу в умовах застосування атаки ДКП і квантування з шагом $q = 0; 1; 5$.

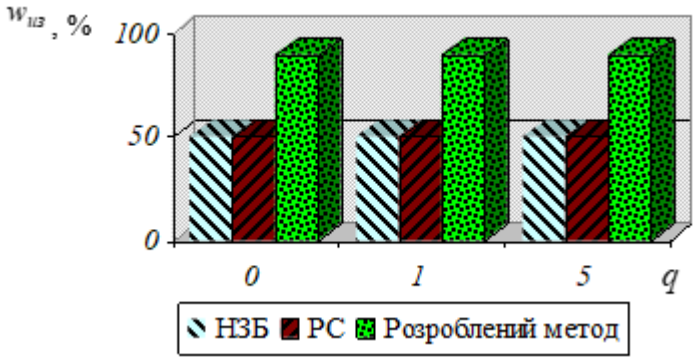

Рисунок 6.16 - Діаграма значень величини $w_{из}^{(m)}$ для методу НЗБ, РС і розробленого методу залежно від типу атак

З аналізу рис. 6.16 можна зробити наступні висновки:

1) для досліджуваних значень коефіцієнтів квантування кількість $w_{из}^{(m)}$ безпомилково вилучених бітів для розробленого методу набуває значень не менше 90 %;

2) в умовах застосування активних атак виграш для розробленого методу відносно методів НЗБ і РС по кількості безпомилково вилучених даних складає 40 %.

6.5 Оцінка стеганографічного бітрейта розробленої стеганографічної системи

Для розробленої системи безпосереднього вбудовування оцінимо величину стеганографічного бітрейта, який визначається на основі наступного виразу:

$$S_b = \lim_{\substack{P_{из}\to 1 \\ h\to\infty}} (f(w_{встр}, Z_{стр}Z_{стб}, P_{из}, h)) , \quad (6.2)$$

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:

$$S_b = \frac{w_{встр}}{Z_{стр}Z_{стб}} , \quad (6.3)$$

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. 6.17 представлена діаграма залежності величини $S_b^{(m)}$ стеганографічного бітрейта розробленої стеганографічної системи від різної довжини m=2;3;4;6 сформованих нерівновагових позиційних чисел.

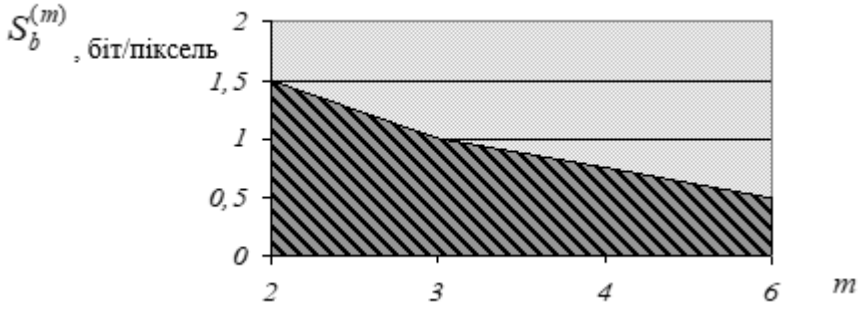

Рисунок 6.17 - Залежність величини $S_b^{(m)}$ стеганографічного бітрейта розробленого методу від довжини m НПЧ

З аналізу діаграми на рис. 6.17 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. 6.18 – 6.20 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. 6.18 – 6.20 можна зробити наступні висновки:

1) 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;

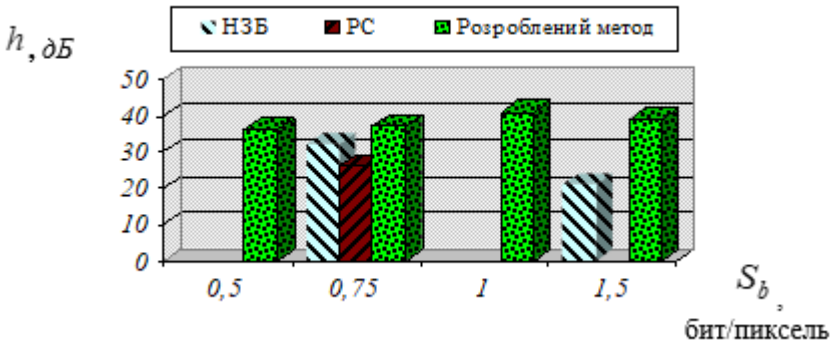

Рисунок 6.18 - Діаграма значень величини S_b і h для сильно насиченого зображення, декодованого на основі методу НЗБ, РС і розробленого методу

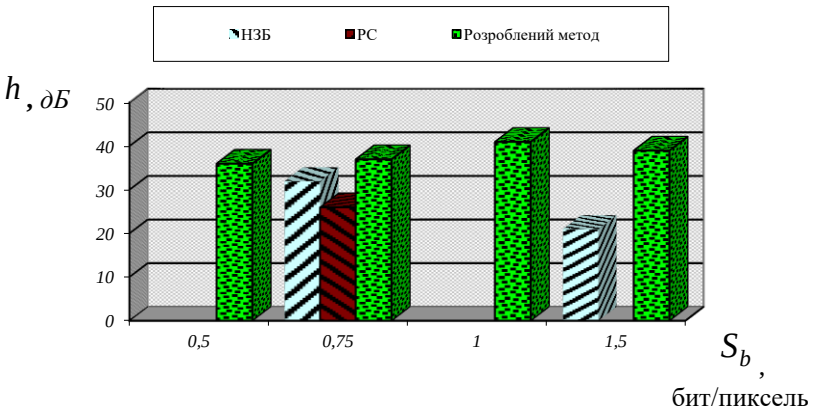

Рисунок 6.19 - Діаграма значень величини S_b і h для середньо насиченого зображення, декодованого на основі методу НЗБ, РС і розробленого методу

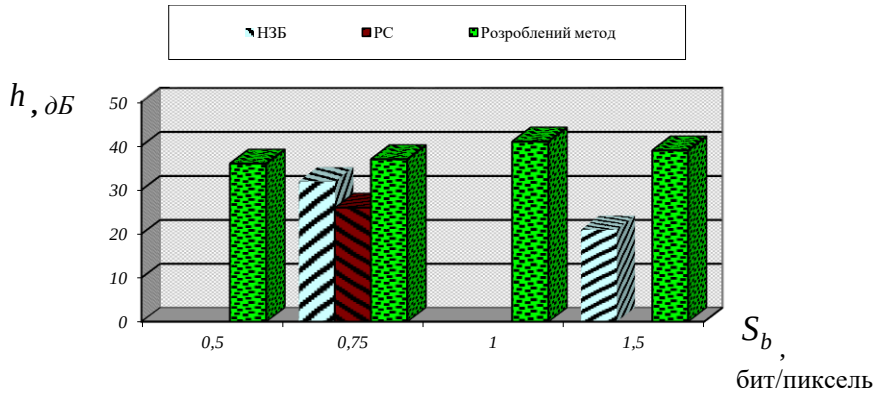

Рисунок 6.20 - Діаграма значень величини S_b і h для слабо насиченого зображення, декодованого на основі методу НЗБ, РС і розробленого методу

З аналізу діаграм на рис. 6.18 – 6.20. можна зробити наступні висновки:

1) 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;

2) 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. Обґрунтований підхід на основі нерівновагового позиційного кодування, де як елемент-контейнер пропонується використовувати нерівновагове позиційне число, а як функціональне перетворення використовується кодоутворювальна функція для нерівновагового позиційного числа. При такому підході передбачається вбудовування біта секретного повідомлення у вихідне нерівновагове позиційне число. В результаті застосування прямого функціонального перетворення для вихідного числа з вбудованою інформацією формується результуюче кодове представлення. Зворотне функціональне перетворення здійснюватиметься для зловмисника (неавторизований доступ) і для авторизованого користувача. При першому способі реконструкція елементу вихідного зображення реалізується неавторизованим користувачем з врахуванням відкритої службової інформації. Другий спосіб дозволяє, за наявності службової інформації і закритого ключа, вилучити біт вбудованих даних і безпомилково реконструювати вихідний елемент зображення-контейнера.

2. Розроблена стеганографічна система на основі прямого і зворотнього функціонального перетворення для нерівновагового позиційного числа з імплантованим елементом, що забезпечує вбудовування і вилучення приховуваної інформації на основі відповідного структурно-комбінаторного стеганографічного кодування і декодування.

3. Розроблено структурно-комбінаторне стеганографічне кодування з маскуванням, що базується на наступних етапах:

- формування нерівновагового позиційного базису для фрагмента зображення;

- структурно-комбінаторне стеганографічне кодування в нерівноваговому базисі основ;

- маскування структурної стеганографічної надлишковості шляхом її

локалізації на основі корекції довжини стеганограми.

4. Створено правило вбудовування інформації для структурно-комбінаторного стеганографічного кодування, яке полягає в тому, що:

1) один біт приховуваного повідомлення вбудовується на старшу позицію нерівновагового позиційного числа;

2) локалізація стеганографічної надлишковості досягається на основі відсікання молодшого біта стеганограми.

На основі правила побудовано маскувальне стеганографічне кодування для вбудовування одного біта на старшу позицію нерівновагового позиційного числа. Це забезпечує вбудовування приховуваної інформації в умовах:

1) підвищення стійкості приховуваної інформації;

2) забезпечення відновлення елементів вихідної відеопослідовності незалежно від наявності вбудованої інформації;

3) зниження кількості структурної стеганографічної надлишковості.

5. Розроблено демаскуюче стеганографічне декодування для витягання імплантованого на старшу позицію біта з одночасною реконструкцією елементів вихідного нерівновагового позиційного числа. Механізм демаскуючого стеганографічного декодування передбачає:

1) відновлення вихідної довжини для скоректованого в процесі маскування стеганокоду;

2) структурно-комбінаторне стеганографічне декодування, що забезпечує відновлення нерівновагового позиційного числа з імплантованим елементом;

3) вилучення елементу приховуваного повідомлення із старшої позиції нерівновагового позиційного числа.

Наукова новизна обумовлена рішенням науково-прикладного завдання підвищення безпеки спеціальних інформаційних ресурсів на основі використання технології структурно-комбінаторного стеганографічного кодування.

Наукова новизна результатів досліджень полягає в тому, що:

1. Вперше розроблена стеганографічна система на основі безпосереднього вбудовування приховуваної інформації у відеопослідовність. На відміну від інших стеганосистем забезпечується одночасне вбудовування і витягання прихованої інформації відповідно в процесі формування і реконструкції кода-контейнера в базисі основ нерівновагового позиційного числа. Це забезпечує вбудовування прихованої інформації на основі обліку кількості структурно-комбінаторної надлишковості фрагментів відеозображень.

2. Вперше розроблений метод структурно-комбінаторного стеганографічного кодування з маскуванням. На відміну від інших методів забезпечується вбудовування приховуваної інформації в процесі нерівновагового позиційного кодування з подальшою локалізацією стеганографічної надлишковості. Це дозволяє знизити можливість виявлення зловмисником факту наявності вбудованої інформації.

3. Вперше розроблено метод демаскуючого стеганографічного декодування. На відміну від існуючих методів витягання прихованої інформації і відновлення нерівновагового позиційного числа проводиться на основі реконструкції стеганокоду за біполярним принципом з демаскуванням стеганографічної надлишковості. Це дозволяє підвищити ефективність витягання приховуваної інформації і локалізувати атаки зловмисника на виявлення факту наявності прихованої інформації.

4. Отримали подальше удосконалення методів підвищення безпеки державної інформації на основі застосування стеганографічних систем. На відміну від інших систем використовується структурно-комбінаторне стеганографічне маскуюче і демаскуюче перетворення. Це дозволяє підвищити скритність і цілісність вбудованої інформації.

Новизна отриманих результатів підтверджується відсутністю розроблених методів в існуючих стандартах цифрової обробки зображень і стеганографічного кодування.

Основні практичні результати полягають в тому, що:

Розроблений метод підвищення безпеки спеціальних інформаційних ресурсів в системах кризового призначення на основі структурно-комбінаторного стеганографічного кодування, доведений до програмно – апаратних реалізацій. На основі чого отримані такі результати:

1. Проведений порівняльний аналіз значень відносної стеганографічної ємності розробленого методу відносно методів найменш значимого біта і розширення спектру показав, що:

1) при однакових значення стеганографічної ємності виграш для розробленого методу відносно методу НЗБ по величині пікового відношення сигнал шум складає в середньому від 8 до 20 дБ.

2) для розробленого методу виграш в значенні стеганографічної ємності відносно методу РС складає від 1,22 до 5,47 %.

2. Оцінка характеристик приховання вбудованих повідомлень в разі неавторизованого доступу дозволяє зробити висновок, що величина ПВСШ для всіх типів зображення набуває максимального значення в разі вбудовування в нерівновагове позиційне число довжиною $m = 2$. При цьому виграш в значенні ПВСШ відносно вбудовування в НПЧ з довжиною $m = 2; 3; 4; 6$ буде рівний:

- для сильно насиченого зображення «Знімок аеропорту» від 2,725 дБ до 4,86 дБ;

- для середньо насиченого зображення «Фотознімок» від 2,71 до 4,79 дБ;

- для слабо насиченого зображення «Літак на фоні неба» від 2,85 до 4,79дБ.

3. Проведений порівняльний аналіз розробленого методу відносно методів НЗБ і РС по ймовірності безпомилкового вилучення вбудованих даних показав, що виграш в значенні ймовірності безпомилкового вилучення відносно методів найменш значимого біта і розширення спектру складає:

- для методу НЗБ - 40 %;

- для методу РС - 50 %.

4. Оцінка стійкості приховуваних повідомлень до атак зловмисника дозволяє зробити висновок, що для різних значень коефіцієнта квантування найбільшою стійкістю володіють дані, стеганографічно вбудовані в нерівновагове позиційне число довжиною $m=6$. Навпаки найменшою стійкістю володіють дані стеганографічно вбудовані в НПЧ довжиною $m=2$. При цьому виграш для розробленого методу відносно методів РС і НЗБ по кількості безпомилково вилучених даних складає:

- відносно методу НЗБ- 40 %;
- відносно методу РС – 40%.

5.Оцінка стеганографічного бітрейта розробленого методу вбудовування дозволяє зробити висновок, що найбільшого значення стеганографічний бітрейт набуває в разі формування нерівновагових позиційних чисел довжиною $m=2$ - 1,5 біта на піксель, і навпаки найменше значення пропускної спроможності спостерігається для нерівновагових позиційних чисел довжиною $m=6$ - 0,5 біта на піксель. При цьому виграш для розробленого методу відносно існуючих методів складає:

- для методу НЗБ – до 25 %;
- для методу РС – до 25 %.

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 неравновесного 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. / 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. . / 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. / 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. / 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. / 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. / Д. В. Бараннік[и др.] // Kharkiv National University of Radio Electronics.— 2016.

7. Метод снижения информационной интенсивности достаточно информативных сегментов аэрофотоснимка. / 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.

/ Д. В. Бараннік[и др.] // Наукоємні технології // 33.1— 2017- С. 46-52.

9. Метод кодування ресурсних блоків для технології 5G. / Д. В. Бараннік[и др.] // Наукоємні технології // 37.1— 2018.

10. Технология балансированной обработки динамического видеоресурса для снижения информационной интенсивности в инфокоммуникационных системах. / 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. / Д. В. Бараннік[и др.] //Радиоэлектроника и информатика // 1 - Харьковский национальный университет радиоэлектроники.— 2017.

12. Метод локализации потери целостности информации на основе слот-технологии. / Д. В. Бараннік[и др.] // Радиоэлектроника и информатика // 4 - Харьковский национальный университет радиоэлектроники.— 2015.

13. Обоснование подхода для формирования квантованного описания трансформанты сегмента аэрофотоснимка. / Д. В. Бараннік[и др.] // Автоматизированные системы управления и приборы автоматики // 173 - Харьковский национальный университет радиоэлектроники.— 2015.

14. Стеганографическая система на основе неравновесного позиционного кодирования. / Д. В. Бараннік[и др.] // Радиоэлектроника и информатика // 4 - Харьковский национальный университет радиоэлектроники.— 2014.

15. Концепция структурного стеганографического кодирования с маскированием. / Д. В. Бараннік[и др.] // Автоматизированные системы управления и приборы автоматики // 168 - Харьковский национальный университет радиоэлектроники.— 2014.

16. Метод криптокомпрессионных преобразований с ключом. / Д. В. Бараннік[и др.] // Сучасна спеціальна техніка // 1 - Міністерство внутрішніх справ України, Державний науково-дослідний інститут МВС України.— 2018 – С. 51 - 57..

Додаток А

Приклади вихідних реалістичних зображень

Рисунок А.1 – Вихідне зображення-контейнер «Знімок аеропорту»

Рисунок А.2– Вихідне зображення-контейнер «Фотознімок»

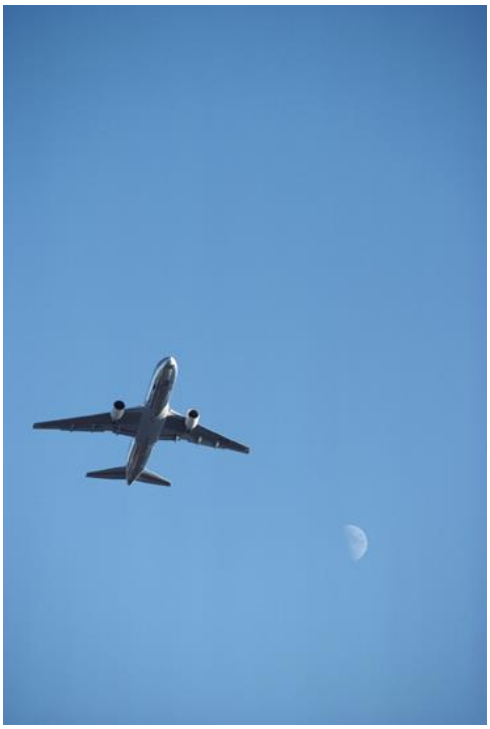

Рисунок А.3 – Вихідне зображення-контейнер «Літак на фоні неба»

Додаток Б

Лістинг

Лістинг Б.1 – ConvertorDefault.kt

```
package ImageCompressionLib.Convertor

import ImageCompressionLib.Containers.*
import ImageCompressionLib.Containers.Type.ByteVector
import ImageCompressionLib.Containers.Type.MyBufferedImage
import ImageCompressionLib.ProcessingModules.ModuleCompression
import ImageCompressionLib.ProcessingModules.ModuleDCT
import ImageCompressionLib.ProcessingModules.ModuleImage
import ImageCompressionLib.ProcessingModules.ModuleOpc
import ImageCompressionLib.Utils.Objects.TimeManager


class ConvertorDefault (val dao: IDao,val guard:IGuard) {
    interface IDao{
        fun onResultByteVectorContainer(vector: ByteVectorContainer)
        fun onResultImage(image: MyBufferedImage, parameters: Parameters)
        fun getImage():Pair<MyBufferedImage, Parameters>
        fun getByteVectorContainer():ByteVectorContainer
    }
    interface IGuard{
        fun getEncryptProperty():EncryptParameters?
        fun onMessageRead(vector: ByteVector)
    }
    //TODO compression utils


    enum class Computing{OneThread,MultiThreads,MultiProcessor}

    fun FromBmpToBar(computing: Computing = Computing.MultiThreads) {
        TimeManager.Instance.startNewTrack("direct")
        val isAsync=(computing== Computing.MultiThreads)
        val (bmp,parameters)= dao.getImage()
        onProgress(10,"RGB to YcBcR")
        onImageReadyListener?.invoke(bmp)
        val mi = ModuleImage(bmp, parameters)
        val matrix = mi.getTripleShortMatrix(isAsync)
        onProgress(30,"direct DCT")
        val bodum = ModuleDCT(matrix)
        val matrixDCT=bodum.getDCTMatrix(isAsync)
        onProgress(60,"direct OPC")
        val moduleOPC= ModuleOpc(matrixDCT)
        val box=moduleOPC.getTripleDataOpcMatrix(guard.getEncryptProperty())
        onProgress(70,"toBV")
        val bvc=box.toByteVectorContainer();
        onProgress(80,"Compress")
        val bvcComp=ModuleCompression().compress(bvc,parameters.flag);
        onProgress(80,"write to file")
        dao.onResultByteVectorContainer(bvcComp)
        TimeManager.Instance.append("Finish")
        onProgress(100,"Ready after ${TimeManager.Instance.getInfoInSec()}")
    }
```

```
    fun FromBarToBmp(computing: Computing = Computing.MultiThreads): Unit {
        TimeManager.Instance.startNewTrack("reverce")
        val isAsync=(computing== Computing.MultiThreads)
        onProgress(10,"read vector from file")
        val bvcComp=dao.getByteVectorContainer()
        onProgress(15,"decompress")
        val
bvc=ModuleCompression().decompress(bvcComp,bvcComp.parameters.flag);
        onProgress(20,"fromBV")
        val box=TripleDataOpcMatrix.valueOf(bvc)
        val parameters=box.parameters
        onProgress(30,"reverse OPC")
        val mOPC= ModuleOpc(box)
        val (FFTM,message)
=mOPC.getTripleShortMatrix(guard.getEncryptProperty())
        message?.let {
            onProgress(40,"setMessage")
            guard.onMessageRead(message)
        }
        onProgress(50,"reverse DCT")
        val bodum1 = ModuleDCT(FFTM)
        val matrixYBR=bodum1.getYCbCrMatrix(isAsync)
        onProgress(70,"YcBcR to BMP");
        val af = ModuleImage(matrixYBR);
        val res = af.getBufferedImage(isAsync)
        onProgress(90,"Write to BMP");
        dao.onResultImage(res,parameters)
        TimeManager.Instance.append("Finish")
        onProgress(100,"Ready after ${TimeManager.Instance.getInfoInSec()}");
        onImageReadyListener?.invoke(res)
    }


    var progressListener:((value:Int,text:String)->Unit)?=null
    var onImageReadyListener:((image: MyBufferedImage)->Unit)?=null

    private fun onProgress(value: Int,s:String){
        progressListener?.invoke(value,s)
        TimeManager.Instance.append(s)
    }
}
```

Лістинг Б.2 – DataOpc.kt

```
package ImageCompressionLib.Containers.Type

import ImageCompressionLib.Constants.ICopyble
import ImageCompressionLib.Containers.Parameters
import java.math.BigInteger
import java.util.*
import kotlin.experimental.and

class DataOpc :ICopyble{
    var base: ShortArray
    var sign: Array<BooleanArray>
    var DC: Short
    var N: BigInteger
    var vectorCode: Vector<Long>
    private val size:Size
    constructor(parameters: Parameters){
        base = ShortArray(parameters.unitSize.height){1.toShort()}
        sign = Array(parameters.unitSize.width) {
```

```
BooleanArray(parameters.unitSize.height) }
        DC = 0
        N = BigInteger("0")
        vectorCode = Vector()
        size=parameters.unitSize
    }
    constructor(unitSize: Size){
        base = ShortArray(unitSize.height){1.toShort()}
        sign = Array(unitSize.width) { BooleanArray(unitSize.height) }
        DC = 0
        N = BigInteger("0")
        vectorCode = Vector()
        size=unitSize
    }
    constructor(DC: Short, N: BigInteger, vectorCode: Vector<Long>,base:
ShortArray, sign: Array<BooleanArray>) {
        this.base = base
        this.sign = sign
        this.DC = DC
        this.N = N
        this.vectorCode = vectorCode
        size=Size(sign.size,sign[0].size)
    }


    fun FromBigIntToVector(vector: ByteVector, length:Int) {
        val code = N.toByteArray()
//        vector.append((short)code.length);
//        var length = getLengthOfCode(base)
        var len=length
        while (len-- > code.size)
            vector.append(0.toByte())

        for (b in code) {
            vector.append(b)
        }
    }
    fun FromVectorToBigInt(vector: ByteVector, length: Int) {
//        int len=vector.getNextShort();
//        val len = getLengthOfCode(base)
        val len =length
        val code = ByteArray(len)
        for (i in 0 until len) {
            code[i] = vector.getNext()
        }
        N = BigInteger(code)
    }


    fun FromSignToVector(vector: ByteVector) {
        for (i in 0 until size.width) {
            for (j in 0 until size.height) {
                vector.append(sign[i][j])
            }
        }
    }
    fun FromVectorToSign(vector: ByteVector) {
        for (i in 0 until size.width) {
            for (j in 0 until size.height) {
                sign[i][j] = vector.getNextBoolean()
            }
        }
    }
```

```
    fun FromBaseToVector(vector: ByteVector, flag: Flag) {
        if(!flag.isChecked(Flag.Parameter.ByteBase)) {//if (!DC)
            for(i in 0 until size.height)
                vector.append(base[i])
        }else{
            for(i in 0 until size.height) {
                vector.append(base[i].toByte())
//                if(base[i]>=0xff)
//                    throw Exception("base[$i]=${base[i]}")
            }
        }
    }
    fun FromVectorToBase(vector: ByteVector, flag: Flag) {
        if(!flag.isChecked(Flag.Parameter.ByteBase)) {//if (!DC)
            for(i in 0 until size.height)
                base[i]=vector.getNextShort();
        }else{
            for(i in 0 until size.height) {
                base[i] = vector.getNext().toShort() and 0xff;
                if(base[i]<=0)
                    base[i]=256
            }
        }
    }

    fun FromDcToVector(vector: ByteVector) {
        vector.append(DC)
    }
    fun FromVectorToDc(vector: ByteVector) {
        DC = vector.getNextShort()
    }

    fun FromCodeToVector(vector: ByteVector) {
        val len = vectorCode.size
//        assert(len < 0xf)
        vector.append(len.toByte())
        for (l in vectorCode) {
            vector.append(l)
        }
    }
    fun FromVectorToCode(vector: ByteVector) {
        val len = vector.getNext().toInt() and 0xFF
        for (i in 0 until len) {
            vectorCode.add(vector.getNextLong())
        }
    }

    fun toByteVector(vector: ByteVector, parameters: Parameters): ByteVector
{
        val f=parameters.flag
        if (f.isChecked(Flag.Parameter.DC))
            FromDcToVector(vector)

        if (!f.isChecked(Flag.Parameter.GlobalBase) &&
f.isChecked(Flag.Parameter.OneFile))
            FromBaseToVector(vector,f)

        if (f.isChecked(Flag.Parameter.LongCode))
            FromCodeToVector(vector)
        else
            FromBigIntToVector(vector, getLengthOfCode(base,
```

```
parameters.unitSize))

        if(f.isChecked(Flag.Parameter.DCT))
            FromSignToVector(vector)

        return vector
    }
    fun setFrom(vector: ByteVector, parameters: Parameters): DataOpc {
        val f = parameters.flag
        if (f.isChecked(Flag.Parameter.DC))
            FromVectorToDc(vector)

        if (!f.isChecked(Flag.Parameter.GlobalBase) &&
f.isChecked(Flag.Parameter.OneFile))
            FromVectorToBase(vector,f)

        if (f.isChecked(Flag.Parameter.LongCode))
            FromVectorToCode(vector)
        else
            FromVectorToBigInt(vector, getLengthOfCode(base,
parameters.unitSize))

        if(f.isChecked(Flag.Parameter.DCT))
            FromVectorToSign(vector)

        return this
    }


    fun assertEquals(other: Any?): Boolean {
        if (this === other)
            return true
        if (other!!.javaClass != DataOpc::class.java)
            throw Exception("other class ${other!!.javaClass}")//return false

        val d = other as DataOpc?
        if (d!!.DC != DC)
            throw Exception("DC: ${DC}!=${d.DC}")//return false
        for (i in 0 until base.size) {
            if (d.base[i] != base[i])
                throw Exception("base[$i]: ${base[i]}!=${d.base[i]}")//return
false
            for (j in 0 until sign[0].size) {
                if (d.sign[i][j] != sign[i][j])
                    throw Exception("sign[$i][$j]:
${sign[i][j]}!=${d.sign[i][j]}")//return false
            }
        }
        if (d.vectorCode.size != vectorCode.size)
            throw Exception("vectorCode.size not equals")//return false

        for (i in vectorCode.indices) {
            if (d.vectorCode[i] != vectorCode[i])
                throw Exception("code[$i]:
${vectorCode[i]}!=${d.vectorCode[i]}")//return false
        }

        if(N.compareTo(d.N)!=0)
            throw Exception("BI: $N!=${d.N}")

        return true
    }
    override fun equals(other: Any?): Boolean {
```

```
        if (this === other) return true
        if (javaClass != other?.javaClass) return false

        val d=other as DataOpc

        if (d!!.DC != DC)
            return false
        for (i in 0 until base.size) {
            if (d.base[i] != base[i])
                return false
            for (j in 0 until sign.size) {
                if (d.sign[j][i] != sign[j][i])
                    return false
            }
        }
        if (d.vectorCode.size != vectorCode.size)
            return false

        for (i in vectorCode.indices) {
            if (d.vectorCode[i] != vectorCode[i])
                return false
        }
        if(N.compareTo(d.N)!=0)
            throw Exception("BI: $N!=${d.N}")


        return true
    }

    override fun hashCode(): Int {
        var result = Arrays.hashCode(base)
        result = 31 * result + Arrays.hashCode(sign)
        result = 31 * result + DC
        result = 31 * result + N.hashCode()
        result = 31 * result + vectorCode.hashCode()
        return result
    }
    override fun copy(): DataOpc {
        val rN= BigInteger(N.toByteArray())
        val rDC=DC
        val rbase=ShortArray(base.size){base[it]}
        val rsign=Array(sign.size){i->BooleanArray(sign[0].size){j-
>sign[i][j]}}
        val rcode=Vector<Long>()
        for(el in this.vectorCode)
            rcode.addElement(el)

        return DataOpc(rDC, rN, rcode, rbase, rsign)
    }

    fun getByteSize(parameters: Parameters): Int {
        val vector = ByteVector(10)
        toByteVector(vector, parameters)
        return vector.size
    }

    override fun toString(): String {
        return "DataOpc(base=${Arrays.toString(base)}, DC=$DC, N=$N,
sign=${Arrays.toString(sign)}, vectorCode=$vectorCode)"
    }


    companion object {
```

```
        //support utils
        private fun getLengthOfCode(base: ShortArray,unitSize: Size): Int
{//TODO optimize this fun
            var bi = BigInteger("1")
            for (i in 0 until unitSize.width) {
                for (j in 0 until unitSize.height)
                    bi = bi.multiply(BigInteger.valueOf(base[j].toLong()))
            }
            return bi.toByteArray().size
        }

        @JvmStatic
        fun valueOf(byteVector: ByteVector, parameters: Parameters): DataOpc
{
            val dataOpc = DataOpc(parameters)
            dataOpc.setFrom(byteVector,parameters)
            return dataOpc
        }
    }
}
```

Лістинг Б.3 – OpcConvertor.kt

```
package ImageCompressionLib.Utils.Objects

import ImageCompressionLib.Containers.*
import ImageCompressionLib.Containers.Matrix.DataOpcMatrix
import ImageCompressionLib.Containers.Matrix.Matrix
import ImageCompressionLib.Containers.Matrix.ShortMatrix
import ImageCompressionLib.Containers.Type.ByteVector
import ImageCompressionLib.Containers.Type.DataOpc
import ImageCompressionLib.Containers.Type.Flag
import ImageCompressionLib.Containers.Type.Size
import ImageCompressionLib.Utils.Functions.Opc.OpcProcess
import ImageCompressionLib.Utils.Functions.Opc.OpcUtils

class OpcConvertor {
    enum class State {
        Opc, Origin
    }
    //TODO replace forEach with for()
    //TODO do all process in one loop

    private val shortMatrix: Matrix<Short>
    private val dataOpcMatrix: DataOpcMatrix
    private val parameters:Parameters
    var isReady = false
        private set
    var state: State
        private set

    private lateinit var splitedShortMatrix: Matrix<Matrix<Short>>
//    private lateinit var splitedDataOpcMatrix:Matrix<DataOpcMatrix>//TODO
make local


    constructor(dataOrigin: Array<Array<Short>>, parameters: Parameters) {
        this.shortMatrix = ShortMatrix.valueOf(dataOrigin)
        this.parameters=parameters
        state = State.Origin
        val
size=calculataDataOpcMatrixSize(Size(dataOrigin.size,dataOrigin[0].size),para
```

```
meters.unitSize)
        dataOpcMatrix= DataOpcMatrix(size.width, size.height,
parameters.unitSize)
    }
    constructor(dataOrigin: ShortMatrix, parameters: Parameters) {
        this.shortMatrix = dataOrigin
        this.parameters=parameters
        state = State.Origin
        val
size=calculataDataOpcMatrixSize(dataOrigin.size,parameters.unitSize)
        dataOpcMatrix= DataOpcMatrix(size.width, size.height,
parameters.unitSize)
    }


    constructor(dataOpcMatrix: DataOpcMatrix, parameters: Parameters){
        this.dataOpcMatrix= (dataOpcMatrix)
        this.parameters=parameters
        state = State.Opc
        val
size=calculateShortMatrixSize(dataOpcMatrix.size,parameters.unitSize)
        shortMatrix= ShortMatrix(size.width, size.height)
    }
    private fun createSplitedMatrix(){
        if(!parameters.flag.isChecked(Flag.Parameter.Enlargement))

splitedShortMatrix=shortMatrix.split(parameters.unitSize.width,parameters.uni
tSize.height)
        else

splitedShortMatrix=shortMatrix.splitWithZeroIterator(parameters.unitSize.widt
h,parameters.unitSize.height,0)
    }
    private fun calculataDataOpcMatrixSize(imageSize: Size, unitSize:Size):
Size {
        var w= imageSize.width/unitSize.width
        var h= imageSize.height/unitSize.height
        if(imageSize.width%unitSize.width!=0)w++
        if(imageSize.height%unitSize.height!=0)h++
        return Size(w, h)
    }
    private fun
calculateShortMatrixSize(dataOpcMatrixSize:Size,unitSze:Size): Size {
        return
Size(dataOpcMatrixSize.width*unitSze.width,dataOpcMatrixSize.height*unitSze.h
eight)
    }
    private fun beforDirectOpc(){
        dataOpcMatrix.forEach() { i, j, value ->
            OpcProcess.preDirectOpcProcess(parameters, splitedShortMatrix[i,
j], value)
            return@forEach null
        }
    }
    private fun afterReverceOpc(){
        dataOpcMatrix.forEach() { i, j, value ->
            OpcProcess.afterReverceOpcProcess(parameters,value,
splitedShortMatrix[i, j])
            return@forEach null
        }
    }
    private fun setGlobalBase(){
//        if(!parameters.flag.isChecked(Flag.Parameter.GlobalBase))
```

```
//            return
        val
splitedDataOpcMatrix=dataOpcMatrix.split(parameters.sameBaseSize.width,parame
ters.sameBaseSize.height)
        splitedDataOpcMatrix.forEach(){i, j, value ->
            OpcUtils.setSameBaseIn(value)
            return@forEach null
        }
    }
    private fun directOpc(){
        dataOpcMatrix.forEach(){i, j, value ->
            OpcProcess.directOPC(parameters, splitedShortMatrix[i,j],value)
            return@forEach null
        }
    }
    private fun reverceOPC(){
        dataOpcMatrix.forEach(){i, j, value ->
            OpcProcess.reverseOPC(parameters,value, splitedShortMatrix[i,j])
            return@forEach null
        }
    }
    private fun directOpcWithMessageAt(encParameters: EncryptParameters,
message: ByteVector){
        if(encParameters.steganography==null)
            throw Exception("steganography==null")
        val position= encParameters.steganography!!.stegoPosition
        val stegoGeter=
encParameters.steganography!!.stegoBlockKeygenFactory.invoke()
        dataOpcMatrix.forEach(){i, j, value ->
            if(message.hasNextBit()&&stegoGeter.isUseNextBlock())
                OpcProcess.directOpcWithMessageAt(parameters,
splitedShortMatrix[i,j] ,value,message.getNextBoolean(),position)
            else
                OpcProcess.directOpcWithMessageAt(parameters,
splitedShortMatrix[i,j] ,value,false,position)
            return@forEach null
        }
    }
    private fun reverceOPCWithMessageAt(encParameters: EncryptParameters):
ByteVector {
        val res= ByteVector()
        if(encParameters.steganography==null)
            throw Exception("steganography==null")
        val position= encParameters.steganography!!.stegoPosition
        val stegoGeter=
encParameters.steganography!!.stegoBlockKeygenFactory.invoke()
        dataOpcMatrix.forEach(){i, j, value ->
            val tmp=OpcProcess.reverseOpcWithMessageAt(parameters,value,
splitedShortMatrix[i,j] ,position)
            if(stegoGeter.isUseNextBlock())res.append(tmp)
            return@forEach null
        }
        encParameters.message=res
        return res
    }
    private fun directProcess(encParameters: EncryptParameters?, message:
ByteVector?){
        createSplitedMatrix()

        beforDirectOpc()

        if(parameters.flag.isChecked(Flag.Parameter.GlobalBase))
            setGlobalBase()
```

```
        if(encParameters?.steganography!=null&&message!=null)
            directOpcWithMessageAt(encParameters,message)
        else
            directOpc()
    }
    private fun reverceProcess(encParameters: EncryptParameters?):
ByteVector?{
        createSplitedMatrix()

        var res: ByteVector?=null
        if(encParameters?.steganography!=null)
            res = reverceOPCWithMessageAt(encParameters)
        else
            reverceOPC()

        afterReverceOpc()

        return res
    }


    fun getDataOrigin(encParameters: EncryptParameters?=null):
Pair<Matrix<Short>,ByteVector?> {
        var m:ByteVector?=null
        if (state == State.Opc && !isReady) {
            m=reverceProcess(encParameters)
            isReady = true
        }

        return Pair(shortMatrix,m)
    }

    /**
     * calculate(if need) DataOpcs with global base for (nxm)
     * @param n - vertical size of same base
     * @param m - horizonlat size of same base
     * @return matrix of DataOpcOld with same base
     */
    fun getDataOpcs(): Matrix<DataOpc> {
        if (state == State.Origin && !isReady) {
            directProcess(null,null)
            isReady = true
        }
        return dataOpcMatrix
    }
    fun getDataOpcs(encParameters: EncryptParameters?,message:ByteVector?):
Matrix<DataOpc> {
        if (state == State.Origin && !isReady) {
            directProcess(encParameters,message)
            isReady = true
        }
        return dataOpcMatrix
    }
}
```

№	Позначення	Найменування	Дод. відомості
		Текстові документи	
1	ГЮІК.504300.036 ПЗ	Пояснювальна записка	__ с.
		Графічні документи	
2		Демонстраційні матеріали	__ слайдів
		Носії інформації	
3		Компакт-диск (CD)	1 шт.

Змін.	Арк.	Номер докум.	Підп.	Дата	ГЮІК.504300.036 ПЗ			
Розроб.		Бараннік Д.В.			Структурно-стеганографічне кодування з плаваючим базисом вбудовування для підвищення безпеки інформаційних ресурсів Відомість атестаційної роботи	Літ	Аркуш	Аркушів
Перевір.		Литвинова Є.І.				У	1	1
Н.контр.		Філіпенко І.В.				ХНУРЕ Кафедра АПОТ		
Затв.		Чумаченко С. В.						