РОЗДІЛ 3. КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Соколов Артем Вікторович
д.т.н., проф., професор кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

Евдокимов Денис Віталійович
аспірант кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

КОНЦЕПЦІЯ КОДОВОГО УПРАВЛІННЯ У ЦИФРОВІЙ СТЕГАНОГРАФІЇ: ТЕОРЕТИЧНІ ОСНОВИ, РЕАЛІЗАЦІЇ ТА ПЕРСПЕКТИВИ

DOI https://doi.org/10.36059/978-966-397-537-5-6

1.1. Вступ і постановка задачі

Однією з ключових складових сучасних систем захисту інформації, зокрема при її передаванні за допомогою сучасних телекомунікаційних систем, є стеганографічні методи, що дозволяють приховати сам факт передачі секретної інформації [1]. Розвиток кіберпростору у бік багаторазового збільшення обсягів переданої мультимедійної інформації, а також поява пристроїв IoT і мобільних пристроїв [2–4], що володіють високими вимогами до обчислювальної ефективності застосовуваних методів, дозволяють сформулювати ключові вимоги до стеганографічних методів: висока надійність сприйняття стеганоповідомлення; стійкість стеганоповідомлення до атак проти вбудованого повідомлення, в першу чергу, атак стисненням із втратами; висока швидкодія та простота алгоритмічної реалізації.

Для забезпечення високої стійкості стеганографічного методу до атак стисненням, вбудовування інформації має відбуватися в низькочастотні та середньочастотні складові контейнера [5], що найбільш просто зробити із застосуванням областей перетворення контейнера:

дискретного косинусного перетворення (ДКП), вейвлет-перетворення, спектрального/сингулярного розкладання матриць блоків контейнера. Наслідком цієї обставини є те, що більшість відомих сьогодні стеганографічних методів, що позиціонуються як стійкі до атак проти вбудованого повідомлення [6–15] виконують операції вбудовування та вилучення інформації у зазначених областях перетворень. Тим не менш, використання областей перетворення контейнера для стеганоперетворення призводить до ускладнення алгоритмічної реалізації стеганографічних методів, до збільшення обчислювальної складності за рахунок наявності переходів з просторової області в область перетворення та назад, а також, часто, до неконтрольованих змін яскравості пікселів зображення у просторовій області, що може привести до погіршення надійності сприйняття стеганоповідомлення [1].

Принципова перспективність використання просторової області для вбудовування інформації була обґрунтована в роботі [16], тим не менш, до розробки концепції кодового управління, реалізація відповідності стеганографічного метода основним критеріям ефективності була утруднена.

Проривом стало створення концепції кодового управління вбудовуванням додаткової інформації [17], яка отримала свій подальший розвиток у роботах [18–20]. Зазначена концепція дозволяє здійснювати контроль за вбудовуванням додаткової інформації у ту або іншу частотну складову без необхідності здійснення затратного з обчислювальної точки зору переходу в області перетворень.

Метою дослідження є аналітичне узагальнення результатів, отриманих авторами у рамках розробки концепції кодового управління в цифровій стеганографії, із подальшим обґрунтуванням ефективності відповідних методів в умовах практичних атак і обмежень сучасних інформаційних систем.

Зважаючи на поставлену мету сформулюємо задачі дослідження:

1. Проаналізувати сучасні підходи до вбудовування додаткової інформації в цифрові контейнери з позицій стійкості до атак, надійності сприйняття та обчислювальної ефективності.

2. Систематизувати основні положення концепції кодового управління в цифровій стеганографії, зокрема у контексті використання досконалих алгебраїчних конструкцій.

3. Оцінити переваги та обмеження використання просторової області зображення для вбудовування інформації без необхідності переходу до частотної області.

4. Узагальнити та формалізувати результати, отримані в рамках класичного стеганографічного методу з кодовим управлінням.

5. Узагальнити та формалізувати результати стосовно стеганографічного методу з кодовим управлінням та можливістю сліпого декодування.

6. Узагальнити та формалізувати підходи до побудови стеганографічного методу з кодовим управлінням на основі досконалих двійкових решіток.

7. Визначити перспективні напрямки подальшого розвитку концепції кодового управління в умовах сучасних викликів інформаційної безпеки.

Об'єкт дослідження – процеси стеганографічного перетворення в цифрових контейнерах.

Предмет дослідження – методи стеганографічного вбудовування з використанням концепції кодового управління, зокрема їх теоретичні засади, кодові конструкції, властивості стійкості, надійності та можливість сліпого декодування.

Розглянемо далі основні наявні сьогодні теоретичні та практичні здобутки, отримані під час розвитку цієї концепції, а також основні проблеми, які необхідно вирішити для подальшого розвитку та практичного впровадження концепції кодового управління.

1.2. Основні визначення

Коротко розглянемо основні визначення, які застосовуються в роботі.

У сучасних методах цифрової стеганографії важливу роль відіграють перетворення зображень у частотну область, які дозволяють досягти високої непомітності та стійкості прихованої інформації. Одним із найпоширеніших таких перетворень є дискретне косинусне перетворення (ДКП) [21], що широко використовується в алгоритмах стиснення зображень (наприклад, JPEG) і є природним середовищем для приховування даних. Перехід до частотного представлення зображення дозволяє обирати зони з меншою чутливістю зорової системи людини для модифікації, знижуючи ризик візуального або статистичного виявлення. Матриця трансформант S ДКП визначається за допомогою наступного співвідношення:

$$S = C_N X C_N^T, C_N = \left\| c_{i,j} \right\|, i, j = 0,1,..., N-1, c_{i,j} =$$
$$= \begin{cases} \dfrac{1}{\sqrt{N}}, & \text{при } i = 0; \\ \sqrt{\dfrac{2}{N}} \cos\left(\dfrac{(2j+1) \cdot i \cdot \pi}{2N} \right), & \text{при } i > 0, \end{cases} \quad (1)$$

де X – фрагмент вихідного зображення розміру $N \times N$.

Перетворенням, яке покладено в основу стеганографічного методу з кодовим управлінням вбудовуванням інформації є двовимірне перетворення Уолша – Адамара. Окрім класичних частотних методів, у стеганографії набувають популярності альтернативні ортогональні перетворення, зокрема перетворення Уолша – Адамара [22]. Це перетворення базується на використанні функцій, що приймають лише два значення (±1), і не потребує операцій множення, що забезпечує його високу обчислювальну ефективність. Завдяки своїй простоті, перетворення Уолша – Адамара є привабливим для реалізації у системах з обмеженими ресурсами, а також дає можливість створювати ефективні алгоритми вбудовування інформації зі збереженням високої швидкодії. Матриця трансформант W для перетворення Уолша – Адамара визначаються за допомогою наступного співвідношення:

$$W = H'_N X H'^T_N, H'_N = \frac{1}{\sqrt{N}} H_N, H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{bmatrix}, H_1 = [1], \quad (2)$$

де H_N і H'_N – ненормована та нормована матриці Уолша – Адамара порядку $N \times N$, відповідно.

Вектор трансформант V одновимірного перетворення Уолша – Адамара вектора Y довжини N визначається за допомогою наступного співвідношення:

$$V = YH_N. \quad (3)$$

Одним з теоретичних здобутків, який лежить в основі концепції кодового управління вбудовуванням інформації є встановлений в роботі [23] взаємозв'язок між трансформантами двовимірного та одновимірного перетворення Уолша – Адамара, який може бути

записаний (з точністю до коефіцієнта $1/N$) за допомогою оператора $\tilde{A}$, який визначає запис матриці A порядку $N \times N$ у вигляді вектору-рядка довжини N^2 шляхом послідовної конкатенації рядків вихідної матриці A:

$$\tilde{W} = \tilde{X} H_{N^2}, \tag{4}$$

при цьому вираз (4) є справедливим і для інших видів перетворень, насамперед, ДКП, однак, замість матриці H_{N^2} в цьому випадку має застосовуватися матриця $A1_{N^2}$, що побудована відповідно до [23].

Реалізація основної ідеї кодового управління вбудовуванням інформації, яка була запропонована у роботі [17] зводиться до додавання матриць блоків контейнера і кодових слів, елементи яких належать алфавіту $\{\pm 1\}$, тоді блок стеганоповідомлення, а також, із врахуванням (4), його трансформанти перетворення Уолша – Адамара визначається як

$$\begin{gathered} M = X + T, \\ \tilde{M} H_{N^2} = (\tilde{X} + \tilde{T}) H_{N^2} = \tilde{X} H_{N^2} + \tilde{T} H_{N^2}, \end{gathered} \tag{5}$$

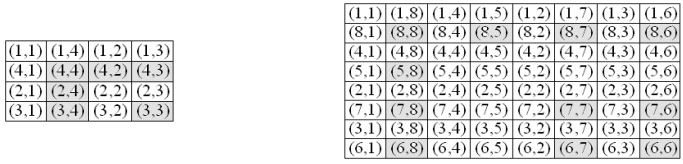
де M – блок стеганоповідомлення розміру $\mu \times \mu$, T – кодове слово розміру $\mu \times \mu$, елементи якого $t_{i,j} \in \{\pm 1\}, i, j = 1, 2, ..., \mu$.

З виразу (5) безпосередньо витікає той факт, що підбираючи такі кодові слова T, які характеризуються впливом на ті чи інші трансформанти перетворення Уолша – Адамара можна забезпечити строго заданий вплив на необхідні трансформанти перетворення Уолша – Адамара контейнера, таким чином, отримуючи задані властивості стеганоповідомлення M. В якості таких кодових слів T було запропоновано застосування $N \times N$-матричного подання рядків матриці Уолша – Адамара порядку N^2, тобто коду Ріда – Маллера першого порядку.

Беручи до уваги теоретичні результати роботи [23], можемо сформулювати дві достатні умови, які є основою для побудови кодових слів, що застосовуються у стеганографічних методах, заснованих на концепції кодового управління.

Достатня умова забезпечення надійності сприйняття стеганоповідомлення. Для забезпечення надійності сприйняття стеганоповідомлення достатньо проводити вбудовування додаткової інформації

таким чином, щоб в області перетворення Уолша – Адамара його результатом було збурення елементів, локалізація яких наведена на рис. 1. для $l \times l$-блоків розміру $l \in \{4,8,16\}$, при цьому саме вбудовування ДІ може здійснюватися не тільки безпосередньо в області Уолша – Адамара, а й у будь-якій іншій області контейнера (просторовій, перетворення). При необхідності використання блоків іншого розміру рекомендується проводити вбудовування ДІ таким чином, щоб результатом його було збурення елементів в області перетворення Уолша – Адамара в межах другого стовпця та другого рядка перетвореної матриці.



(1,1)	(1,4)	(1,2)	(1,3)
(4,1)	(4,4)	(4,2)	(4,3)
(2,1)	(2,4)	(2,2)	(2,3)
(3,1)	(3,4)	(3,2)	(3,3)

а

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

б

(1,1)	(1,16)	(1,8)	(1,9)	(1,4)	(1,13)	(1,5)	(1,12)	(1,2)	(1,15)	(1,7)	(1,10)	(1,3)	(1,14)	(1,6)	(1,11)
(16,1)	(16,16)	(16,8)	(16,9)	(16,4)	(16,13)	(16,5)	(16,12)	(16,2)	(16,15)	(16,7)	(16,10)	(16,3)	(16,14)	(16,6)	(16,11)
(8,1)	(8,16)	(8,8)	(8,9)	(8,4)	(8,13)	(8,5)	(8,12)	(8,2)	(8,15)	(8,7)	(8,10)	(8,3)	(8,14)	(8,6)	(8,11)
(9,1)	(9,16)	(9,8)	(9,9)	(9,4)	(9,13)	(9,5)	(9,12)	(9,2)	(9,15)	(9,7)	(9,10)	(9,3)	(9,14)	(9,6)	(9,11)
(4,1)	(4,16)	(4,8)	(4,9)	(4,4)	(4,13)	(4,5)	(4,12)	(4,2)	(4,15)	(4,7)	(4,10)	(4,3)	(4,14)	(4,6)	(4,11)
(13,1)	(13,16)	(13,8)	(13,9)	(13,4)	(13,13)	(13,5)	(13,12)	(13,2)	(13,15)	(13,7)	(13,10)	(13,3)	(13,14)	(13,6)	(13,11)
(5,1)	(5,16)	(5,8)	(5,9)	(5,4)	(5,13)	(5,5)	(5,12)	(5,2)	(5,15)	(5,7)	(5,10)	(5,3)	(5,14)	(5,6)	(5,11)
(12,1)	(12,16)	(12,8)	(12,9)	(12,4)	(12,13)	(12,5)	(12,12)	(12,2)	(12,15)	(12,7)	(12,10)	(12,3)	(12,14)	(12,6)	(12,11)
(2,1)	(2,16)	(2,8)	(2,9)	(2,4)	(2,13)	(2,5)	(2,12)	(2,2)	(2,15)	(2,7)	(2,10)	(2,3)	(2,14)	(2,6)	(2,11)
(15,1)	(15,16)	(15,8)	(15,9)	(15,4)	(15,13)	(15,5)	(15,12)	(15,2)	(15,15)	(15,7)	(15,10)	(15,3)	(15,14)	(15,6)	(15,11)
(7,1)	(7,16)	(7,8)	(7,9)	(7,4)	(7,13)	(7,5)	(7,12)	(7,2)	(7,15)	(7,7)	(7,10)	(7,3)	(7,14)	(7,6)	(7,11)
(10,1)	(10,16)	(10,8)	(10,9)	(10,4)	(10,13)	(10,5)	(10,12)	(10,2)	(10,15)	(10,7)	(10,10)	(10,3)	(10,14)	(10,6)	(10,11)
(3,1)	(3,16)	(3,8)	(3,9)	(3,4)	(3,13)	(3,5)	(3,12)	(3,2)	(3,15)	(3,7)	(3,10)	(3,3)	(3,14)	(3,6)	(3,11)
(14,1)	(14,16)	(14,8)	(14,9)	(14,4)	(14,13)	(14,5)	(14,12)	(14,2)	(14,15)	(14,7)	(14,10)	(14,3)	(14,14)	(14,6)	(14,11)
(6,1)	(6,16)	(6,8)	(6,9)	(6,4)	(6,13)	(6,5)	(6,12)	(6,2)	(6,15)	(6,7)	(6,10)	(6,3)	(6,14)	(6,6)	(6,11)
(11,1)	(11,16)	(11,8)	(11,9)	(11,4)	(11,13)	(11,5)	(11,12)	(11,2)	(11,15)	(11,7)	(11,10)	(11,3)	(11,14)	(11,6)	(11,11)

в

Рисунок 1 – Локалізація області можливого збурення в результаті стеганоперетворення в області перетворення Уолша – Адамара для $l \times l$-блоків цифрового зображення: а – $l = 4$; б – $l = 8$; в – $l = 16$

Достатня умова забезпечення нечутливості стеганоповідомлення до збурних дій. Для забезпечення нечутливості стеганоповідомлення до збурних дій достатньо проводити вбудовування

додаткової інформації таким чином, щоб в області перетворення Уолша – Адамара його результатом було збурення елементів, локалізованих як

ДКП	Перетворення Уолша-Адамара
$(1,1);\ (1,2);\ (2,1);$ $(3,1);\ (2,2);\ (1,3)...$	$4\times4:(1,1);\ (1,3);\ (3,1);\ (4,1);\ (3,3);\ (1,4)...$ $8\times8:(1,1);\ (1,5);\ (5,1);\ (7,1);\ (5,5);\ (1,7)...$ $16\times16:(1,1);\ (1,9);\ (9,1);\ (13,1);\ (9,9);\ (1,13)...$

, (6)

для $l\times l$-блоків розміру $l\in\{4,8,16\}$, при цьому саме вбудовування додаткової інформації може здійснюватися не тільки безпосередньо в області Уолша – Адамара, а й у будь-якій іншій області контейнера (просторовій, перетворення).

На практиці стеганографічні методи, побудовані на принципах кодового управління, характеризуються тим, що вплив на кожен окремий піксель контейнера обмежується зміною не більше ніж на ±1. Такий рівень модифікації є практично непомітним для людського зору, що забезпечує високу надійність візуального сприйняття модифікованого зображення. Відтак, основна увага при конструюванні кодових слів у межах таких методів зосереджується не на зменшенні помітності, а на максимізації стійкості до атак, спрямованих на виявлення або спотворення вбудованого повідомлення. Це визначає специфіку побудови кодів – вони мають бути не лише компактними, а й адаптованими до типових деструктивних впливів (наприклад, стиснення, фільтрації або статистичного аналізу).

З практичної точки зору інтерес являє побудова кодових слів різної довжини, насамперед практично важливих довжин 4×4, 8×8, що змінюють лише ті складові контейнеру, які були отримані у достатній умові забезпечення надійності стеганоповідомлення до збурних впливів.

Відповідно до встановленої відповідності між двовимірним і одновимірним перетворенням Уолша – Адамара в якості таких кодових слів візьмемо 5, 33, 37 і 1-ший рядки матриці Уолша – Адамара порядку $N^2=64$ (у вигляді відповідних їм матриць порядку $N=8$), для кожної з яких наведемо відповідну матрицю трансформант Уолша – Адамара (з точністю до коефіцієнта $1/N$).

$$T_1^+ = \begin{bmatrix} 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \end{bmatrix}, \quad W_1^+ = \begin{bmatrix} 0&0&0&0&64&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix};$$

$$T_2^+ = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ -1&-1&-1&-1&-1&-1&-1&-1 \\ -1&-1&-1&-1&-1&-1&-1&-1 \\ -1&-1&-1&-1&-1&-1&-1&-1 \\ -1&-1&-1&-1&-1&-1&-1&-1 \end{bmatrix}, W_2^+ = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 64&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}; \quad (7)$$

$$T_3^+ = \begin{bmatrix} 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ 1&1&1&1&-1&-1&-1&-1 \\ -1&-1&-1&-1&1&1&1&1 \\ -1&-1&-1&-1&1&1&1&1 \\ -1&-1&-1&-1&1&1&1&1 \\ -1&-1&-1&-1&1&1&1&1 \end{bmatrix}, W_3^+ = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&64&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix};$$

$$T_4^+ = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}, \quad W_4^+ = \begin{bmatrix} 64&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}.$$

У сучасних стеганографічних методах на основі кодового управління переважна більшість підходів використовує кодові слова, які впливають вибірково лише на одну трансформанту перетворення Уолша – Адамара, наприклад, кодові слова (7). Така стратегія дозволяє імплементувати досить прості та зрозумілі методи синтезу кодових слів, забезпечуючи як високу надійність сприйняття так і стійкість до атак проти вбудованого повідомлення. Проте вона має і суттєве обмеження – низьку інформаційну щільність, оскільки для

вбудовування одного біта інформації зазвичай використовується один блок або навіть одна трансформанта. Водночас можливість паралельного впливу кодових слів на кілька трансформант перетворення Уолша–Адамара відкриває потенціал для значного підвищення пропускної спроможності та стійкості до атак стеганоаналізу, особливо якщо вплив реалізується з урахуванням спектральних або кореляційних властивостей сигналу.

Однак синтез таких складних багатоканальних кодових конструкцій залишається майже недослідженою сферою. Вона потребує нових підходів до проєктування кодів із заданими спектральними характеристиками, здатних одночасно керувати групою трансформант без істотного порушення статистичних або візуальних параметрів контейнера. Це, зокрема, передбачає створення моделей залежностей між трансформантами, розробку метрик взаємного впливу та оптимізаційних критеріїв для балансування між непомітністю, стійкістю та пропускною спроможністю. Розвиток цього напряму відкриває перспективи для побудови високоефективних адаптивних методів стеганографії, здатних протистояти сучасним стеганоаналітичним атакам.

У наступних підрозділах буде детально проаналізовано три найбільш ефективні та практично значущі стеганографічні методи, що реалізують концепцію кодового управління: класичний метод, метод із сліпим декодуванням, а також перспективний метод, побудовану на основі досконалих двійкових решіток.

1.3. Класичний стеганографічний метод з кодовим управлінням

Класичний стеганографічний метод з кодовим управлінням [17] ґрунтується на надзвичайно елегантному та водночас ефективному принципі: приховане повідомлення вбудовується в контейнер шляхом адитивного накладення кодового слова на блок даних. У цьому підході кожен інформаційний біт визначає вибір конкретного кодового слова з заздалегідь заданого коду, яке потім додається до блоку контейнера (наприклад, трансформант або просторових значень). Завдяки цьому забезпечується керованість модифікацій,

передбачуваність структури спотворень і висока стеганографічна непомітність. Метод є не лише концептуально прозорим, а й надзвичайно гнучким: він легко адаптується до різних доменів перетворень, дозволяє реалізувати рівномірний розподіл змін, а також створює підґрунтя для подальших вдосконалень, зокрема в напрямку адаптивних схем і побудови спеціалізованих кодів з потрібними властивостями.

Вбудовування додаткової інформації

Крок 1. Виконуємо сегментацію вихідного зображення P розміру $m \times n$ на блоки $\mu \times \mu$.

Крок 2. Кожному блоку вихідного зображення розміру $\mu \times \mu$, задіяному в процесі стеганоперетворення, ставимо у відповідність λ біт додаткової інформації, таким чином отримуємо матрицю додаткової інформації D розміру $\frac{m}{\mu} \times \frac{n}{\mu}$, кожен елемент якої містить λ біт інформації. При цьому $\lambda = \log_2 J$, де J – кількість кодових слів, що використовуються.

Крок 3. Будуємо таблицю відповідності половини комбінацій із λ біт додаткової інформації кодовим словам $\{T_i^+\}$, тоді як друга половина комбінацій із λ біт додаткової інформації кодується за допомогою інверсій кодових слів $\{T_i^-\}$. Відзначимо, що така таблиця може бути частиною ключа. Отримуємо закодовану матрицю додаткової інформації шляхом подання кожного її елемента з λ біт додаткової інформації за допомогою кодових слів $\{T_i^+\}$ та $\{T_i^-\}$.

Крок 4. Виконуємо вбудовування інформації шляхом підсумовування матриці контейнера P з кодовою матрицею, що була отримана на *Кроці 3*, в результаті чого отримуємо стеганоповідомлення M, тобто

$$M = P + D. \tag{8}$$

Декодування додаткової інформації

Крок 1. Вилучення інформації відбувається шляхом віднімання з матриці можливо збуреного стеганоповідомлення $\overline{M}$ матриці контейнера P, що є частиною секретного ключа. В результаті вилучення, для кожного i-го блоку розміру $\mu \times \mu$ отримуємо матрицю Δ_i:

$$\{\Delta_i\} = \overline{M} - P,\ i = 0,1,\ldots mn-1. \quad (9)$$

Крок 2. Для кожної матриці T_i^+ робимо поелементне множення кожної отриманої на *Кроці 1* матриці Δ_i на матрицю T_i^+, після чого знаходимо суму всіх елементів результуючої матриці кожного кодового слова T_i^+, тобто розраховуємо значення:

$$\sigma_j = \sum_{l=0}^{\mu-1}\sum_{k=0}^{\mu-1}\Delta_i(l,k)T^+(l,k),\ j = 0,1,\ldots,J/2-1.$$

Крок 3. Серед отриманої для кожного блоку множини значень σ_i знаходимо максимальне за модулем значення. При цьому індекс знайденого значення буде відповідати індексу декодованого кодового слова $T_i^?$, в той час як знак знайденого максимуму буде відповідати знаку, з яким вказане кодове слово було вбудовано (прямий або інверсний вигляд).

Зазначимо, що *Крок 2* та *Крок 3* у частині декодування додаткової інформації в представленому методі, по суті, реалізують алгоритм оптимального прийому [24].

Зауваження. Зважаючи на те, що більшість використовуваних зображень сьогодні представлені з використанням моделі RGB, де для кодування кожного кольору відводиться 1 байт (кожна складова кольору представляється числами в діапазоні $[0,...,255]$), у разі наявності в блоці граничних для даного діапазону значень (0 або 255), вказаний блок не використовується в процесі стеганоперетворення у разі застосування розробленого стеганографічного методу.

На рис. 2 представлені графіки залежності кількості помилок, що виникають (у відсотках від загальної кількості біт додаткової інформації) від степеню стиснення *QF* зображення алгоритмом JPEG для кожної з розглянутих трансформант Уолша – Адамара (кодові слова (7) розміру 8×8, а також кодові слова, що одночасно впливають на всі складові блоків контейнера), що дозволяє оцінити ефективність їх використання для протистояння атакам стисненням на стеганоповідомлення. При цьому, через те, що всі кодові слова, які використовують одночасно всі частотні складові показують практично еквівалентні результати, на графіку (рис. 2) вони показані однією кривою.

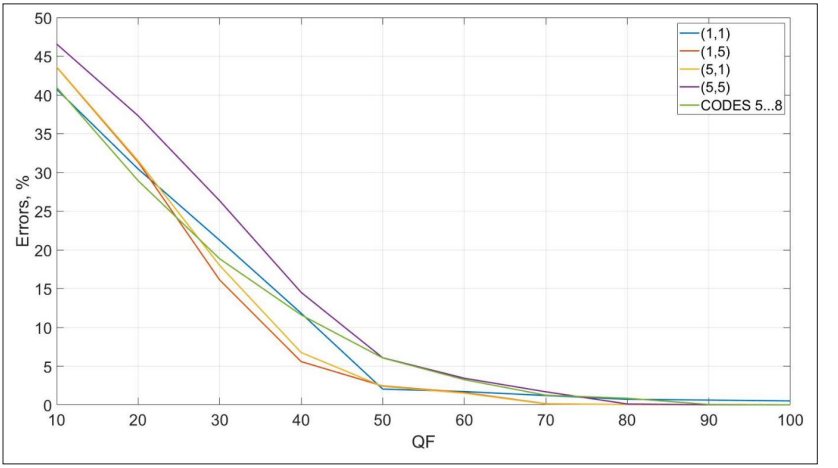


Рисунок 2 – Графік залежності кількості помилок, що виникають, від степеня *QF* стиснення стеганоповідомлення алгоритмом JPEG для різних трансформант Уолша – Адамара, в які здійснюється вбудовування

Аналіз даних, представлених на рис. 2 показує, що вбудовування інформації як з використанням кодових слів (7), так і кодових слів, які використовують одночасно всі частотні складові, формує стеганоповідомлення, нечутливе до атаки стисненням. При цьому, при стисненні з коефіцієнтом $QF = 60\,\%$ (на практиці вкрай нечасто використовуються більші степені стиснення), відсоток помилок, що виникають, не перевищує 5 %, що є показником високої стійкості стеганографічного методу.

На рис. 3 представлено графік залежності кількості помилок при декодуванні вбудованого повідомлення від степеню стиснення стеганоповідомлення алгоритмом JPEG під час проведення атаки для кодових слів розміру 16×16.

Аналіз даних рис. 3 дозволяє дійти висновку, що використання кодових слів розміру 16×16 забезпечує високий рівень стійкості розробленого стеганографічного методу. Так, навіть при атаці з рівнем стиску $QF = 30$ для будь-якого кодового слова кількість помилок при декодуванні не перевищує 5 %. Однак, така стійкість досягається за рахунок зниження пропускної спроможності стеганографічного методу до значення 1/256.

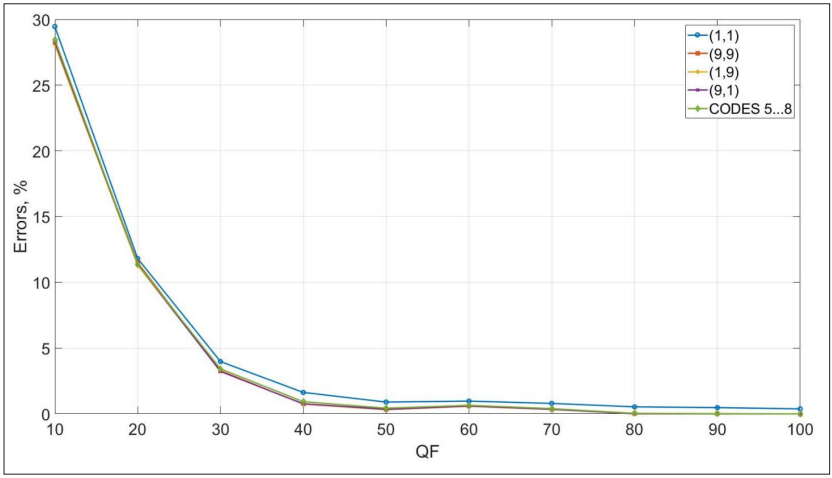
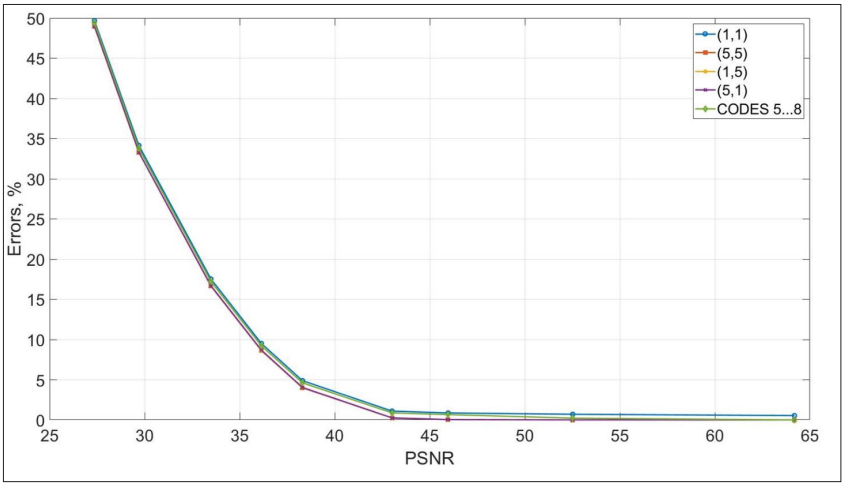


Рисунок 3 – Графік залежності кількості помилок, що виникають, від степеня *QF* стиснення зображеного алгоритмом JPEG для $\mu = 16$

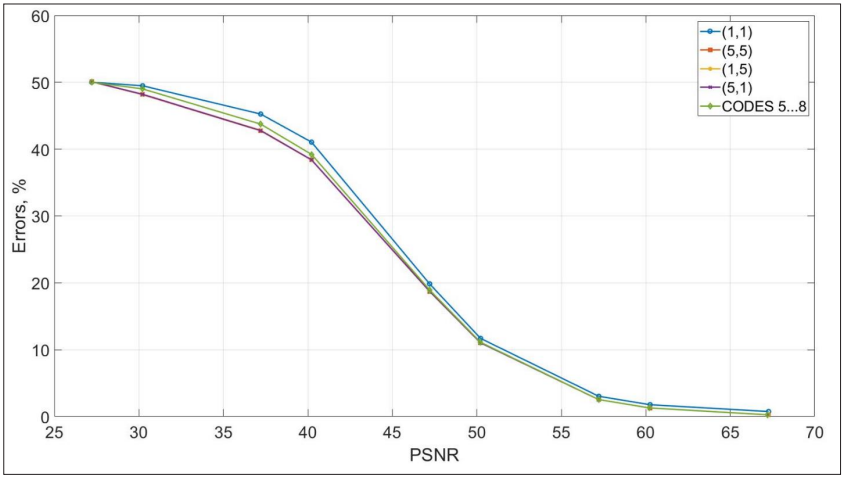
На рис. 4 показано графік залежності кількості помилок при декодуванні додаткової інформації при її вилученні від степеню зашумленості стеганоповідомлення гаусівським шумом (а) та шумом типу “salt&pepper” (б), який виражено у PSNR для блоків розміру 8×8.

Аналіз даних, представлених на рис. 4 показує, що розроблений стеганографічний метод з кодовим управлінням забезпечує рівень стійкості до виникнення помилок у стеганоповідомленні на рівні менше за 5 % при зашумленні гаусівським шумом з PSNR = 43 дБ або зашумленні на рівні PSNR = 57 дБ для випадку шуму “salt&pepper”.

На рис. 5 представлений приклад вбудовування додаткової інформації в контейнер за допомогою розробленого стеганографічного методу, при цьому використані параметри $\lambda = 1$, $\mu = 8$, а також для вбудовування інформації застосовано кодове слово T_2^+. Розмір контейнера становить 2592×3872, при цьому вбудовування інформації відбувалося в кожну колірну складову. Таким чином, загальний обсяг вбудованої інформації для даного контейнера склав 470 448 біт.

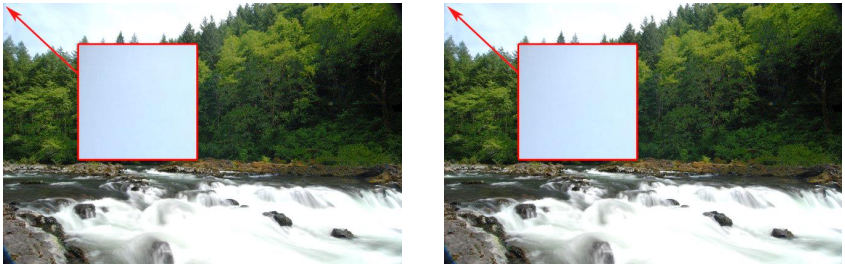


а



б

Рисунок 4 – Графік залежності кількості помилок при декодуванні зашумленого стеганоповідомлення від PSNR при використанні кодових слів розміру 8 × 8: а – зашумлення гаусівським шумом, б – зашумлення шумом типу “salt&pepper”



а б

Рисунок 5 – Приклад використання розробленого стеганографічного методу: а – контейнер; б – стеганоповідомлення

Суб'єктивне ранжування зображень, що представлені на рис. 5 не дозволяє виявити артефакти, або будь-які інші відмінності стеганоповідомлення від вихідного контейнера. Даний факт є очікуваним, оскільки результатом стеганоперетворення є збурення значень яскравості пікселів контейнера на ±1.

Зауваження. Обчислювальна складність алгоритмічної реалізації розробленого методу визначається кількістю блоків, що використовуються в процесі стеганоперетворення, і в найгіршому випадку складе $\underline{O}(nm)$ операцій. З урахуванням блоковості методу очевидним є його внутрішній паралелізм, що разом із використанням просторової області для стеганоперетворення забезпечує потенційну можливість його використання в режимі реального часу для потокового контейнера.

1.4. Стеганографічний метод з кодовим управлінням та сліпим декодуванням

Серед варіацій стеганографічного методу з кодовим управлінням особливе місце посідає модифікація, що забезпечує сліпе декодування [19]. На відміну від класичного методу, який передбачає наявність оригінального контейнера для витягування повідомлення, цей варіант дозволяє відновлювати приховану інформацію без доступу до незміненого зображення, що значно підвищує

практичну гнучкість методу та його придатність для реальних умов застосування.

У стеганографічному методі з кодовим управлінням вбудовуванням додаткової інформації із сліпим декодуванням блок контейнера X застосовується для вбудовування одного біта додаткової інформації d, тоді як зазначений біт розподіляється по підблокам χ_j, $j = 1,2,...,4$. Вбудовування додаткової інформації відбувається у адитивний спосіб, тоді як блок стеганоповідомлення визначатиметься у наступний спосіб:

$$M = X + T_{\mu}, \tag{10}$$

де T_{μ} – кодове слово розміру $\mu \times \mu$, яке формується наступним чином:

$$T_{\mu} = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right] + ... + \left[\begin{array}{c|c} t_n & t_n \\ \hline -t_n & -t_n \end{array}\right], \tag{11}$$

де $t_i, i = 1,2,...,n$ – кодові слова розміру $\mu/2 \times \mu/2$, що мають елементарну структуру [23] перетворення Уолша – Адамара $\left\{(\mu/2)^2(1), 0((\mu/2)^2 - 1)\right\}$, тобто кожне з кодових слів $\left[\begin{array}{c|c} t_i & t_i \\ \hline -t_i & -t_i \end{array}\right]$ при адитивному вбудовуванні (10) здатне забезпечити вибірковий вплив на задану трансформанту перетворення Уолша – Адамара підблоків χ_j, $j = 1,2,...,4$.

Відповідно до [23], для того, щоб кодові слова t_i мали елементарну структуру $\left\{(\mu/2)^2(1), 0((\mu/2)^2 - 1)\right\}$, вони мають бути побудовані шляхом послідовного заповнення відповідної матриці t_i розміру $\mu/2 \times \mu/2$ елементами відповідного рядка матриці Уолша – Адамара $H_{(\mu/2)^2}$.

Твердження 1. Сумарний вплив на трансформанти перетворення Уолша – Адамара підблоків χ_j, $j = 1,2,...,4$ при адитивному вбудовуванні додаткової інформації (10) із застосуванням кодового слова T_{μ} буде визначатися як сума впливів від кожного кодового слова $t_i, i = 1,2,...,n$.

Доказ. Оскільки спосіб розбиття кодового слова T_{μ} на кодові слова $t_i, i = 1,2,...,n$ розміру $\mu/2 \times \mu/2$ відповідає способу розбиття

блоку контейнеру X на підблоки, то можемо представити блок стеганоповідомлення M розміру $\mu \times \mu$ у вигляді наступної конструкції:

$$M = \left[\begin{array}{c|c} m_1 & m_2 \\ \hline m_3 & m_4 \end{array}\right] = \left[\begin{array}{c|c} \chi_1 & \chi_2 \\ \hline \chi_3 & \chi_4 \end{array}\right] + \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right] + \ldots + \left[\begin{array}{c|c} t_n & t_n \\ \hline -t_n & -t_n \end{array}\right], \quad (12)$$

де

$$\begin{cases} m_1 = \chi_1 + t_1 + t_2 + \ldots + t_n; \\ m_2 = \chi_2 + t_1 + t_2 + \ldots + t_n; \\ m_3 = \chi_3 - t_1 - t_2 - \ldots - t_n; \\ m_4 = \chi_4 - t_1 - t_2 - \ldots - t_n, \end{cases} \quad (13)$$

тоді враховуючі (4), трансформанти перетворення Уолша – Адамара підблоків m_1, m_2, m_3, m_4 будуть визначатися як:

$$\begin{aligned} \tilde{W}_{m_1} &= \tilde{W}_{\chi_1} + \tilde{W}_{t_1} + \tilde{W}_{t_2} + \ldots + \tilde{W}_{t_n}; \\ \tilde{W}_{m_2} &= \tilde{W}_{\chi_2} + \tilde{W}_{t_1} + \tilde{W}_{t_2} + \ldots + \tilde{W}_{t_n}; \\ \tilde{W}_{m_3} &= \tilde{W}_{\chi_3} - \tilde{W}_{t_1} - \tilde{W}_{t_2} - \ldots - \tilde{W}_{t_n}; \\ \tilde{W}_{m_4} &= \tilde{W}_{\chi_4} - \tilde{W}_{t_1} - \tilde{W}_{t_2} - \ldots - \tilde{W}_{t_n}, \end{aligned} \quad (14)$$

що доводить Твердження 1.

При цьому, якщо в якості матриць t_i розміру $\mu/2 \times \mu/2$ застосовуються кодові слова, що мають елементарну структуру перетворення Уолша – Адамара $\left\{(\mu/2)^2(1), 0((\mu/2)^2 - 1)\right\}$, результуючий вплив на підблоки χ_j, $j = 1,2,\ldots,4$ розміру $\mu/2 \times \mu/2$ буде складатися із впливів на трансформанти перетворення Уолша – Адамара, що забезпечують застосовані кодові слова t_i.

Твердження 2. Найбільше (за модулем) значення амплітуди впливу кодового слова T_μ на елемент блоку зображення X при застосуванні кодових слів, що засновані на рядках матриці Уолша – Адамара $H_{(\mu/2)^2}$ буде дорівнювати n.

Доказ. Оскільки за побудовою (2) перший стовбець матриці $H_{(\mu/2)^2}$ буде складатися з елементів +1, елементи всіх кодових

слів t_i з індексом (1,1), що побудовані на основі відповідного рядка матриці Уолша – Адамара будуть містити значення +1. Таким чином, у виразі (13), амплітуда максимального значення суми $t_1 + t_2 + \ldots + t_n$, або амплітуда мінімального значення різниці $-t_1 - t_2 - \ldots - t_n$ у позиції (1,1) дорівнюватиме n за модулем, тобто кількості застосованих кодових слів t_i.

Твердження 3. Структура кодового слова T_μ, яка обумовлена впливами кодових слів t_i на трансформанти підблоків $\tilde{W}_{\chi_1}, \tilde{W}_{\chi_2}, \tilde{W}_{\chi_3}, \tilde{W}_{\chi_4}$ блоку X може бути відновлена по блокам стеганоповідомлення m_1, m_2, m_3, m_4 за умови достатньо низького відхилення трансформант перетворення Уолша – Адамара, на які впливають кодові слова t_i підблоків χ_j, $j = 1,2,...,4$ від середнього арифметичного значення відповідних трансформант даних підблоків.

Доказ. Розглянемо вектор, що містить середні арифметичні значення трансформант перетворення Уолша – Адамара:

$$\begin{aligned}\tilde{W}_{\overline{m}} = \frac{1}{4}(\tilde{W}_{m_1} + \tilde{W}_{m_2} + \tilde{W}_{m_3} + \tilde{W}_{m_4}) = \frac{1}{4}(\tilde{W}_{\chi_1} + \tilde{W}_{t_1} + \tilde{W}_{t_2} + \ldots + \tilde{W}_{t_n} + \\ + \tilde{W}_{\chi_2} + \tilde{W}_{t_1} + \tilde{W}_{t_2} + \ldots + \tilde{W}_{t_n} + \tilde{W}_{\chi_3} - \tilde{W}_{t_1} - \tilde{W}_{t_2} - \ldots - \tilde{W}_{t_n} + \\ \tilde{W}_{\chi_4} - \tilde{W}_{t_1} - \tilde{W}_{t_2} - \ldots - \tilde{W}_{t_n}) = \frac{1}{4}(\tilde{W}_{\chi_1} + \tilde{W}_{\chi_2} + \tilde{W}_{\chi_3} + \tilde{W}_{\chi_4}),\end{aligned} \quad (15)$$

які визначаються виключно трансформантами перетворення Уолша – Адамара підблоків χ_j, $j = 1,2,...,4$.

Розглянемо матрицю різниць трансформант перетворення Уолша – Адамара підблоків стеганоповідомлення m_1, m_2, m_3, m_4 і середнього значення $\tilde{W}_{\overline{m}}$.

$$\left[\begin{array}{c|c} \Delta_1 & \Delta_2 \\ \hline \Delta_3 & \Delta_4 \end{array}\right] =$$

$$= \left[\begin{array}{c|c} \tilde{W}_{\chi_1} - \tilde{W}_{\overline{m}} + \tilde{W}_{t_1} + \tilde{W}_{t_2} + \ldots + \tilde{W}_{t_n} & \tilde{W}_{\chi_2} - \tilde{W}_{\overline{m}} + \tilde{W}_{t_1} + \tilde{W}_{t_2} + \ldots + \tilde{W}_{t_n} \\ \hline \tilde{W}_{\chi_3} - \tilde{W}_{\overline{m}} - \tilde{W}_{t_1} - \tilde{W}_{t_2} - \ldots - \tilde{W}_{t_n} & \tilde{W}_{\chi_4} - \tilde{W}_{\overline{m}} - \tilde{W}_{t_1} - \tilde{W}_{t_2} - \ldots - \tilde{W}_{t_n} \end{array}\right]. \quad (16)$$

Неважко побачити, що за виконання умов:

$$\begin{cases} \tilde{W}_{\chi_1} - \tilde{W}_{\overline{m}} \to 0; \\ \tilde{W}_{\chi_2} - \tilde{W}_{\overline{m}} \to 0; \\ \tilde{W}_{\chi_3} - \tilde{W}_{\overline{m}} \to 0; \\ \tilde{W}_{\chi_4} - \tilde{W}_{\overline{m}} \to 0, \end{cases} \quad (17)$$

де під 0 розуміється нульовий вектор порядку $(\mu/2)^2$, матриця $\left[\begin{array}{c|c} \Delta_1 & \Delta_2 \\ \hline \Delta_3 & \Delta_4 \end{array}\right]$ відтворюватиме структуру кодового слова T_μ, що обумовлює принципову можливість його декодування.

Відзначимо, що на практиці для контейнерів, у які відбувається вбудовування додаткової інформації, умова (17) не виконується, що потенційно веде до виникнення помилок при декодуванні кодового слова T_μ. Такі помилки будемо називати обумовленими варіацією підблоків.

Із застосуванням результатів Твердження 1 і Твердження 2 запишемо алгоритм вбудовування додаткової інформації:

Крок 1. Оригінальне зображення розбивається на блоки X_i розміру $\mu \times \mu$ стандартним способом.

Крок 2. У кожен із блоків відбувається вбудовування біта додаткової інформації d_i за допомогою кодового слова T_μ розміру $\mu \times \mu$, тобто i-й блок стеганоповідомлення визначається як

$$M_i = X_i + d_i T_\mu,\ T_\mu = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right] + \ldots + \left[\begin{array}{c|c} t_n & t_n \\ \hline -t_n & -t_n \end{array}\right], \quad (18)$$

де $t_i, i = 1,2,\ldots,n$ – кодові слова розміру $\mu/2 \times \mu/2$, що впливають на обрані трансформанти Уолша – Адамара.

Із застосуванням результатів Твердження 3 запишемо алгоритм вилучення додаткової інформації:

Крок 1. Стеганоповідомлення M' розбити на блоки M'_i розміру $\mu \times \mu$.

Крок 2. Для чергового блоку M'_i розміру $\mu \times \mu$ виконати його розбиття ще на 4 блоки розміру $\mu/2 \times \mu/2$ відповідно до наступної конструкції $M'_i = \left[\begin{array}{c|c} m_1 & m_2 \\ \hline m_3 & m_4 \end{array}\right]$.

Крок 3. Для кожного блоку M_i' розрахувати n матриць розміру 2×2:

$$u_i = \left[\begin{array}{c|c} \sum_{a=1}^{4}\sum_{b=1}^{4} m_1(a,b)t_i(a,b) & \sum_{a=1}^{4}\sum_{b=1}^{4} m_2(a,b)t_i(a,b) \\ \hline \sum_{a=1}^{4}\sum_{b=1}^{4} m_3(a,b)t_i(a,b) & \sum_{a=1}^{4}\sum_{b=1}^{4} m_4(a,b)t_i(a,b) \end{array} \right], i = 1,2,...,n, \quad (19)$$

де запис $m(a,b)$ означає елемент матриці m з індексом (a,b).

Крок 4. Знайти середні значення $\overline{u_i} = \sum_{l=1}^{2}\sum_{m=1}^{2} u_i(l,m), i = 1,2,...,n$.

Крок 5. Знайти значення вилученого біту додаткової інформації для даного блоку M_i' як

$$d_i' = \text{sign}\left(\sum_{i=1}^{n} \left((u_i(1,1) - \overline{u_i}) + (u_i(1,2) - \overline{u_i}) - (u_i(2,1) - \overline{u_i}) - (u_i(2,2) - \overline{u_i}) \right) \right). \quad (20)$$

Зважаючи на зміст Твердження 1 і Твердження 2, а також на практичні результати, які були отримані у [14], доцільним вбачається використання на практиці значення розміру блоку $\mu = 8$ і значення $n = 3$, які розглядаються далі в цій роботі. Тим не менш, питання оптимізації даних параметрів, на думку авторів, становлять окремий інтерес що виходить за рамки представлених у статті результатів.

У стеганографічному методі з кодовим управлінням вбудовуванням додаткової інформації викладеному в [17] в якості кодових слів обґрунтовано використання матричного представлення рядків матриці Уолша – Адамара порядку N^2 і показано, що тільки такі кодові слова забезпечують вибірковий вплив на ту, або іншу трансформанту перетворення Уолша – Адамара.

Зважаючи на те, що кодові слова t_1 і t_2 мають порядок $N = 4$, вони можуть бути побудовані на основі матриці Уолша – Адамара порядку $N^2 = 16$ шляхом представлення її рядків у вигляді матриць розміру 4×4. Покажемо зазначені кодові слова у табл. 1, де для кожного кодового слова зверху зазначено на яку трансформанту Уолша – Адамара воно впливає.

Таблиця 1 – Можливі варіанти кодових слів t_1 і t_2

(1,1)	(1,2)	(1,3)	(1,4)
$\xi_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\xi_2 = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\xi_3 = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\xi_4 = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$
(2,1)	(2,2)	(2,3)	(2,4)
$\xi_5 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\xi_6 = \begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\xi_7 = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\xi_8 = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
(3,1)	(3,2)	(3,3)	(3,4)
$\xi_9 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$	$\xi_{10} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$	$\xi_{11} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$	$\xi_{12} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$
(4,1)	(4,2)	(4,3)	(4,4)
$\xi_{13} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\xi_{14} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$	$\xi_{15} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$	$\xi_{16} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

Для повноти викладу матеріалу розглянемо конкретний приклад. Нехай визначено кодове слово ξ_3, що здійснює зосереджений вплив на трансформанту Уолша – Адамара (1,3). Знайдемо для нього трансформанти перетворення Уолша – Адамара (2) (з точністю до нормувального коефіцієнта $1/N$):

$$W_{\xi_3} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 16 & 0 \\ 0 & \mathbf{0} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (21)$$

Як бачимо з (21), кодове слово ξ_3 дійсно має матрицю трансформант перетворення Уолша – Адамара, що характеризується лише однією ненульовою трансформантою перетворення Уолша – Адамара.

Проведені дослідження дозволили встановити, що при виборі того чи іншого набору кодових слів $\xi_i, \xi_j, i, j = 1,2,...,16$ в якості t_1 і t_2, на результуючу стійкість стеганографічного методу будуть впливати два основних фактори, які розглянемо докладно.

1. Помилки обумовлені варіацією підблоків.

Згідно до алгоритму вилучення додаткової інформації у досліджуваному стеганографічному методі, стеганоповідомлення сегментується на блоки $\mu \times \mu$ після чого кожний отриманий блок додатково сегментується на підблоки $\mu/2 \times \mu/2$, після чого визначення значень елементів вбудованого кодового слова відбувається відповідно до «нульової точки», в якості якої слугують середні значення $\overline{u_i}, i = 1,2,...,n$.

Зважаючи на те, що використовувані у стеганографічному методі кодові слова вибірково впливають на задану трансформанту перетворення Уолша – Адамара, середні значення $\overline{u_i}, i = 1,2,...,n$ по суті являють собою середні значення трансформант Уолша – Адамара, на які впливають кодові слова $t_i, i = 1,2,...,n$. На практиці можливою є ситуація, коли розкид значень даних трансформант Уолша – Адамара у зазначених підблоках розміру $\mu \times \mu$ блоку $\mu/2 \times \mu/2$ перевищує сумарну амплітуду впливу на дану трансформанту кодового слова, що веде до неможливості вилучення додаткової інформації із даного блоку.

Розглянемо конкретний приклад такої ситуації. Нехай задано вихідний блок зображення розміру 8×8:

$$X = \begin{bmatrix} 150 & 143 & 146 & 145 & 142 & 142 & 145 & 144 \\ 129 & 126 & 129 & 132 & 134 & 135 & 132 & 131 \\ 119 & 118 & 120 & 126 & 129 & 129 & 129 & 128 \\ 117 & 121 & 123 & 126 & 129 & 136 & 137 & 132 \\ 121 & 128 & 130 & 132 & 139 & 137 & 139 & 139 \\ 124 & 128 & 133 & 140 & 143 & 137 & 138 & 139 \\ 128 & 128 & 137 & 141 & 138 & 142 & 140 & 138 \\ 129 & 132 & 139 & 138 & 137 & 145 & 142 & 133 \end{bmatrix}, \quad (22)$$

у який необхідно здійснити вбудовування біта додаткової інформації $d = 1$ із застосуванням $n = 2$ однакових кодових слів:

$$t_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, t_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, \quad (23)$$

тобто для вбудовування інформації буде застосовуватися кодове слово:

$$(-1)T_8 = \begin{bmatrix} -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \end{bmatrix}, \quad (24)$$

тоді як стеганоповідомлення матиме вигляд:

$$M = X + (-1)T_8 = \begin{bmatrix} 148 & 141 & 144 & 143 & 140 & 140 & 143 & 142 \\ 127 & 124 & 127 & 130 & 132 & 133 & 130 & 129 \\ 121 & 120 & 122 & 128 & 131 & 131 & 131 & 130 \\ 119 & 123 & 125 & 128 & 131 & 138 & 139 & 134 \\ 123 & 130 & 132 & 134 & 141 & 139 & 141 & 141 \\ 126 & 130 & 135 & 142 & 145 & 139 & 140 & 141 \\ 126 & 126 & 135 & 139 & 136 & 140 & 138 & 136 \\ 127 & 130 & 137 & 136 & 135 & 143 & 140 & 131 \end{bmatrix}. \quad (25)$$

Спробуємо вилучити додаткову інформацію з блоку (25), знаходимо, що

$$u_1 = u_2 = \begin{bmatrix} 98 & 24 \\ -4 & 28 \end{bmatrix}, \quad (26)$$

тоді як середні значення $\overline{u_1} = 36{,}5$ і $\overline{u_2} = 36{,}5$. Таким чином, відповідно до (20) маємо

$$\begin{aligned} d_i' = \operatorname{sign}((98-36{,}5)+(24-36{,}5)-(-4-36{,}5)-(28-36{,}5)+ \\ +(98-36{,}5)+(24-36{,}5)-(-4-36{,}5)-(28-36{,}5))= \\ = \operatorname{sign}(61{,}5-12{,}5+40{,}5+8{,}5+ \\ +61{,}5-12{,}5+40{,}5+8{,}5) = 196. \end{aligned} \quad (27)$$

Як бачимо, суттєва відмінність у значеннях елементів матриць u_1 і u_2 від середніх значень $\overline{u_1}$ і $\overline{u_2}$, яка обумовлена особливостями структури блоку зображення, та перевищує вплив амплітуди кожного з застосованих кодових слів $\left[\begin{array}{c|c} t_i & t_i \\ \hline -t_i & -t_i \end{array}\right]$, призвела до того, що значення результуючої суми під знаком sign стало додатним, що призвело до виникнення помилки при вилученні додаткової інформації.

Таким чином, ризик виникнення помилки існує у тих блоків зображення розміру 8×8, у яких відмінність значень застосованих для вбудовування додаткової інформації трансформант Уолша – Адамара

від середнього значення серед підблоків розміру 4×4 перевищує значення амплітуди впливу кожного з кодових слів $\left[\begin{array}{c|c} t_i & t_i \\ \hline -t_i & -t_i \end{array}\right]$.

Іншими словами, для уникнення ризику помилки при вбудовуванні інформації, середньоквадратичне відхилення δ трансформант Уолша – Адамара, у які відбувається вбудовування інформації, має бути меншим від значення амплітуди впливу кожного з кодових слів $\left[\begin{array}{c|c} t_i & t_i \\ \hline -t_i & -t_i \end{array}\right]$, застосованих для вбудовування інформації.

Для нашого прикладу, вбудовування інформації відбувається із застосуванням кодових слів (23) у трансформанту (3,1). В нашому випадку для блоку (22) маємо наступні значення трансформант (3,1) Уолша – Адамара $[130,56,-36,-4]$, а отже значення середньоквадратичного відхилення складає $\sigma=73{,}073$, що значно перевищує значення 16. Таким чином, блок (22) знаходиться у групі ризику щодо можливого виникнення помилок, пов'язаних із структурними особливостями зображення.

Проведені дослідження дозволили дійти висновку, що для реальних зображень різні трансформанти перетворення Уолша – Адамара характеризуються різними очікуваними значеннями σ. Для оцінки значень σ для різних трансформант Уолша – Адамара був проведений наступний експеримент. Для 500 зображень з бази NRCS [25] у форматі JPEG була виконана сегментація на блоки X_i розміру 4×4, для кожного з яких було знайдено двовимірне перетворення Уолша – Адамара відповідно до (2).

Далі, серед отриманих блоків, була знайдена кількість таких, для яких середньоквадратичне відхилення відповідних трансформант Уолша – Адамара підблоків 4×4 перевищує значення 16, після чого була побудована відповідна стовпчикова діаграма, що показана на рис. 6.

Аналіз даних, представлених на рис. 6 дозволяє дійти висновку про те, що найменшими значеннями кількості блоків із $\sigma\geq16$ володіють трансформанти перетворення Уолша – Адамара із номерами (2,2), (2,4), (4,2), (4,4).

Таким чином, застосування саме даних трансформант Уолша – Адамара для вбудовування додаткової інформації за допомогою стеганографічного методу з кодовим управлінням із сліпим декодуванням дозволить мінімізувати кількість помилок, що обумовлені варіацією підблоків.

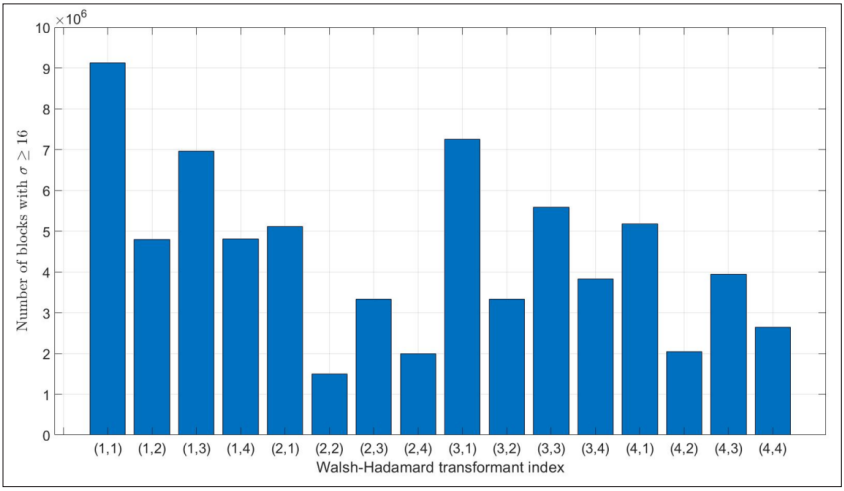


Рисунок 6 – Стовпчикова діаграма, що ілюструє кількості блоків із значенням $\sigma \geq 16$

2. Помилки, що обумовлені атаками проти вбудованого повідомлення. На сьогодні, відомо чимало можливих атак проти вбудованого повідомлення, однак, найбільш розповсюдженою є атака стисненням. Це пояснюється тим, що на практиці зображення нечасто передаються по телекомунікаційним системам або зберігаються у нестисненому вигляді, найчастіше до них застосовуються алгоритми стиску із втратами, найбільш поширеним серед яких є алгоритм JPEG.

Незважаючи на те, що такі алгоритми стиску із втратами, побудовані таким чином, щоб зробити спотворення, що вносяться у зображення найменш помітними людському оку, їх впливу достатньою для знищення додаткової інформації, що вбудована із застосуванням більшості стеганографічних методів, окрім тих, які розроблювалися як стійкі до атак проти вбудованого повідомлення.

Відзначимо, що у відповідності до структури формування кодового слова згідно до (11), отримуємо результуючі кодові слова T_8 при $n=2$, що впливають на відповідні трансформанти перетворення Уолша – Адамара блоку розміру 8×8, при цьому конкретні трансформанти перетворення Уолша – Адамара, на які здійснюють вплив ті чи інші комбінації кодових слів $\xi_i, \xi_i, i = 1,2,...,16$, показані у табл. 2.

Таблиця 2 – Трансформанти Уолша – Адамара, на які здійснюють вплив кодові слова T_8 на основі кодових слів t_1 і t_2

Кодове слово	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7	ξ_8
Трансформанта	(5,1)	(5,2)	(5,3)	(5,4)	(6,1)	(6,2)	(6,3)	(6,4)
Кодове слово	ξ_9	ξ_{10}	ξ_{11}	ξ_{12}	ξ_{13}	ξ_{14}	ξ_{15}	ξ_{16}
Трансформанта	(7,1)	(7,2)	(7,3)	(7,4)	(8,1)	(8,2)	(8,3)	(8,4)

Розглянемо дані, представлені у табл. 2 на конкретному прикладі. Сформуємо із застосуванням формули (11) кодове слово T_8 на основі ξ_3:

$$T_8 = \begin{bmatrix} \xi_3 & \xi_3 \\ -\xi_3 & -\xi_3 \end{bmatrix} + \begin{bmatrix} \xi_3 & \xi_3 \\ -\xi_3 & -\xi_3 \end{bmatrix} = \begin{bmatrix} 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \end{bmatrix}. \quad (28)$$

Знайдемо двовимірне перетворення Уолша – Адамара матриці (28) із застосуванням виразу (2):

$$W_{T_8} = H_8 T_8 H_8^T =$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 & 2 & 2 & -2 & -2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \\ -2 & -2 & 2 & 2 & -2 & -2 & 2 & 2 \end{bmatrix} \times$$

$$\times\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1\\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1\end{bmatrix}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 128 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}. \quad (29)$$

Як бачимо з виразу (29), кодове слово T_8, яке побудоване на основі ξ_3, що впливають на трансформанту (3,1) дійсно забезпечує вплив на трансформанту (5,3), як це показано у табл. 2.

При цьому необхідно зазначити, що одночасне застосування різних кодових слів t_1 і t_2 веде до вбудовування додаткової інформації у відповідну комбінацію трансформант Уолша – Адамара. Наприклад, в разі застосування в якості кодових слів t_1 і t_2 матриць ξ_1 і ξ_9, результуючі кодові слова T_8 будуть виконувати вбудовування додаткової інформації у частотні складові (5,1) і (7,1).

Таким чином, з аналізу даних табл. 2, а також враховуючи достатню умову забезпечення нечутливості стеганоповідомлення до збурних дій можемо прийти до висновку, що найкращими кодовими словами з точки зору стійкості стеганоповідомлення до атаки стиском є, насамперед, кодові слова ξ_1 і ξ_9.

Тим не менш, відповідно до даних табл. 1, кодові слова ξ_1 і ξ_9 впливають на трансформанти Уолша – Адамара (1,1) і (3,1), відповідно, які, згідно до даних рис. 6 мають найбільшу кількість блоків із значенням $\sigma \geq 16$, що ведуть до помилок, обумовлених варіацією підблоків.

І, навпаки, застосування в якості t_1 і t_2 кодових слів ξ_6, ξ_8, ξ_{14} і ξ_{16}, які впливають на трансформанти, що характеризуються найнижчою кількістю блоків із значенням $\sigma \geq 16$ веде до таких результуючих кодових слів T_8, що забезпечують вбудовування додаткової інформації у досить високочастотні трансформанти Уолша – Адамара контейнера (6,2), (6,4), (8,2) і (8,4), відповідно, що не дозволяє забезпечити нечутливість стеганоповідомлення до збурних дій.

Задля практичного підтвердження викладених міркувань, проведемо ряд експериментів.

Для дослідження роботи стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації із сліпим декодуванням під впливом атаки стисненням проти вбудованого повідомлення вбудовування додаткової інформації у 150 випадково обраних зображень з бази NRCS [25] здійснювалося із застосуванням кодових слів T_8^+ і T_8^-, що побудовані на основі двох однакових кодових слів $\xi_i, \xi_i, i = 1,2,...,16$, які використовуються в якості t_1 і t_2. Після вбудовування додаткової інформації зображення піддавалися стисненню алгоритмом JPEG із значеннями $QF = \{100,90,80,70,60,50,40,30,20,10\}$. Далі з атакованого стисненням стеганоповідомлення відбувалося вилучення додаткової інформації із вимірюванням кількості помилок, що відбулися. Результати щодо кількості помилок, що відбулися, для кожного з кодових слів $\xi_i, \xi_i, i = 1,2,...,16$, а також для кожного значення *QF* наведені у табл. 3.

Таблиця 3 – Результати щодо кількості помилок при вилученні додаткової інформації в умовах атаки стисненням алгоритмом JPEG

ξ_i, ξ_j / *QF*	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7	ξ_8	ξ_9	ξ_{10}	ξ_{11}	ξ_{12}	ξ_{13}	ξ_{14}	ξ_{15}	ξ_{16}
100	9,5	0,5	2,6	1,1	2,5	0	0,3	0,1	5,9	0,2	1,7	0,8	2,5	0	0,4	0,2
90	9,6	0,9	2,8	1,2	2,5	0,4	0,8	0,5	5,7	0,4	2,0	1,1	2,5	0,5	0,9	0,6
80	9,8	1,1	3,6	1,6	2,3	24,2	9,4	20,2	6,3	0,8	2,7	2,0	3,0	22,8	4,6	17,5
70	9,8	17,1	4,0	2,5	3,9	27,7	19,3	29,5	6,8	18,9	3,4	3,2	3,1	27,3	16,8	29,6
60	9,9	24,1	4,7	3,3	13,9	29,9	24,7	31,8	7,1	24,7	4,1	10,0	3,6	30,1	25,3	32,0
50	10,3	27,0	5,5	4,9	19,3	31,2	28,3	33,3	7,4	28,0	7,3	29,1	4,6	31,6	28,4	33,4
40	11,2	30,0	9,7	15,4	25,2	33,2	31,1	34,9	8,3	30,8	19,7	33,4	10,7	33,3	31,3	34,7
30	12,6	33,0	24,9	33,0	29,4	35,1	33,9	36,3	9,7	33,9	29,3	35,7	23,0	35,2	34,0	36,4
20	18,7	36,1	33,5	37,9	34,1	37,4	37,0	38,5	21,5	36,8	35,3	38,4	31,5	37,7	37,0	38,5
10	36,0	41,3	40,8	42,5	39,3	41,8	42,1	42,3	37,7	41,6	41,7	42,4	38,7	42,0	41,9	42,5

Аналіз даних, представлених у табл. 3 підтверджує викладені раніше міркування. Так, бачимо, що кодові слова, засновані на матрицях ξ_6, ξ_8 та ξ_{14} показують найкращі результати щодо кількості помилок при вилученні додаткової інформації при значеннях $QF = \{100,90\}$, тобто фактично за умови відсутності атаки проти вбудованої інформації, що пояснюється невеликою кількістю блоків із значенням $\sigma \geq 16$.

З іншого боку, застосування кодових слів ξ_1 та ξ_9, що забезпечують вбудовування додаткової інформації у найбільш низькочастотні для досліджуваного стеганографічного методу компоненти, як бачимо з результатів представлених у табл. 3, найменше збільшують кількість помилок при вилученні додаткової інформації із зменшенням значення *QF*. Тим не менш, велика кількість помилок при декодуванні, що обумовлена варіацією підблоків, не дозволяє рекомендувати їх до практичного застосування. Таким чином, з практичної точки зору, для забезпечення роботи стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації із сліпим декодуванням необхідним є компроміс між мінімізацією кількості помилок, що обумовлені варіацією підблоків (для чого вбудовування додаткової інформації має відбуватися у високочастотні складові) та максимізацією стійкості до збурних дій (для чого вбудовування додаткової інформації має відбуватися у низькочастотні складові блоку). Завдання пошуку такого компромісу вирішується в рамках наступних експериментів.

Наведемо результати дослідження кодового слова, яке дає найкращу стійкість до атаки стисненням, для чого вбудовування додаткової інформації у 150 випадковим чином обраних зображень у форматі JPEG з бази NRCS [25] здійснювалося із застосуванням кодових слів T_8. Кодові слова T_8 складаються з кодових слів t_1, t_2 відповідно до формули $T_8 = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array}\right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array}\right]$, де кодові слова t_1, t_2 розміром $\mu/2 \times \mu/2$ впливають на дві обрані трансформанти Уолша – Адамара (табл. 1). У табл. 4 показані відсотки помилок усіх комбінацій кодових слів t_1 та t_2 при $QF = 70$.

Таблиця 4 – Відсотки помилок усіх комбінацій кодових слів t_1 та t_2

$\xi_i \backslash \xi_j$	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7	ξ_8	ξ_9	ξ_{10}	ξ_{11}	ξ_{12}	ξ_{13}	ξ_{14}	ξ_{15}	ξ_{16}
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ξ_1	9,8	13,9	11,0	10,6	13,2	14,2	13,9	14,1	10,7	13,9	11,8	13,3	10,3	14,2	13,8	14,2
ξ_2	13,8	17,1	7,4	11,8	19,6	25,4	23,2	25,2	10,9	23,5	13,0	23,2	9,0	26,4	25,0	25,4
ξ_3	11,1	7,4	4,1	6,2	9,4	10,1	9,6	10,0	8,2	9,7	6,9	8,9	6,2	10,9	11,6	10,1
ξ_4	10,6	11,8	6,2	2,5	11,0	13,2	11,7	13,9	8,3	11,8	7,4	12,7	6,2	13,2	11,8	18,8
ξ_5	13,2	19,6	9,4	11,1	3,9	21,6	20,1	21,9	9,0	20,2	12,3	19,6	8,4	21,7	20,1	21,9
ξ_6	14,2	25,4	10,1	13,2	21,6	27,7	24,6	29,5	11,6	24,7	10,5	27,0	9,4	29,2	25,7	29,8

Продовження таблиці 4

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ξ_7	13,9	23,2	9,6	11,7	20,1	24,6	19,3	26,0	11,1	21,1	5,8	23,8	8,8	25,9	23,5	26,3
ξ_8	14,1	25,1	10,0	13,9	21,9	29,5	26,1	29,5	11,7	26,0	14,2	15,4	9,3	29,4	25,9	30,9
ξ_9	10,7	10,9	8,2	8,3	9,0	11,6	11,1	11,7	6,8	11,1	8,7	10,5	7,7	11,6	10,9	11,7
ξ_{10}	13,9	23,5	9,7	11,9	20,2	24,6	21,1	26,0	11,1	18,9	7,1	23,9	8,9	26,1	23,4	26,4
ξ_{11}	11,7	13,0	6,9	7,4	12,3	10,5	5,9	14,2	8,7	7,0	3,4	12,9	6,4	14,2	13,1	14,3
ξ_{12}	13,3	23,2	8,8	12,7	19,6	27,0	23,8	15,5	10,5	23,9	12,9	3,2	8,3	26,8	23,8	28,3
ξ_{13}	10,3	9,0	6,2	6,2	8,4	9,4	8,8	9,3	7,7	8,9	6,4	8,3	3,1	9,3	8,6	9,3
ξ_{14}	14,2	26,4	10,8	13,3	21,7	29,2	25,9	29,4	11,6	26,2	14,1	26,9	9,3	27,3	23,8	29,6
ξ_{15}	13,7	25,0	11,6	11,8	20,1	25,7	23,5	25,9	10,9	23,4	13,1	23,8	8,7	23,8	16,8	26,2
ξ_{16}	14,2	25,4	10,1	18,8	21,9	29,8	26,3	30,9	11,7	26,4	14,3	28,2	9,3	29,6	26,2	29,6

Для оцінки рівня стійкості стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації та сліпим декодуванням з бази даних NRCS [25] було випадковим чином обрано 150 зображень у форматі JPEG та проведено подальші експерименти з вилучення додаткової інформації під впливом атаки стисненням за алгоритмом JPEG:

– оригінальний стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації за допомогою кодового слова розміру $\mu = 8$, яке впливає на трансформанту Уолша – Адамара (5,4);

– оригінальний стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації з кодовим словом розміру $\mu = 8$, яке впливає на трансформанту (5,1);

– стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації зі сліпим декодуванням на основі кодових слів ξ_9, ξ_6;

– стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації за допомогою кодових слів, для вибору яких запропоновано обґрунтування: ξ_4, ξ_4, які впливають на трансформанту (5,4), а також на основі кодових слів ξ_7, ξ_{11}, які впливають на трансформанти (6,3) та (7,3).

На рис. 7 наведено графіки залежності кількості помилок, що виникають від степеню стиснення зображення алгоритмом JPEG для всіх розглянутих вище кодових слів, що дозволяє оцінити ефективність їх використання в протистоянні атакам стисненням проти вбудованого повідомлення.

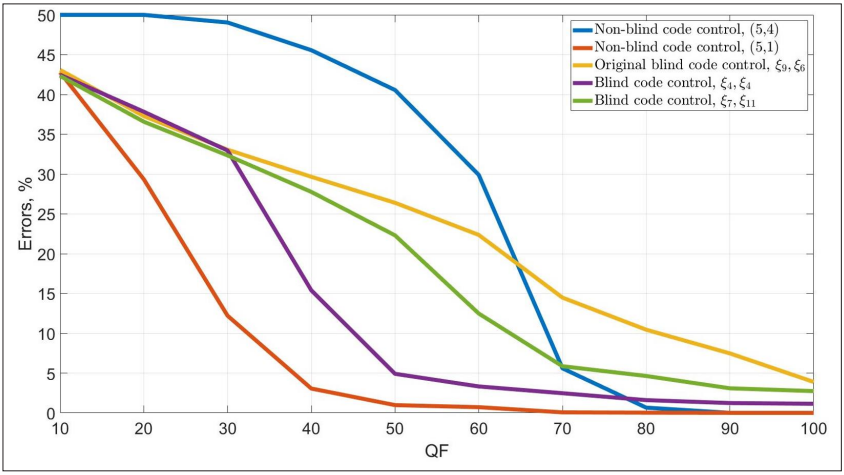


Рисунок 7 – Графік залежності кількості помилок при вилученні додаткової інформації від значення *QF* для стеганографічного методу з кодовим управлінням у різних його варіаціях

Аналіз даних, представлених на рис. 7, показує, що використання кодових слів ξ_4, ξ_4 та ξ_7, ξ_{11} у стеганографічному методі з кодовим управлінням вбудовуванням додаткової інформації та сліпим декодуванням під впливом атаки стисненням JPEG дозволяє зменшити кількість помилок у декодованих значеннях під впливом атаки стисненням JPEG у порівнянні з версією цього методу [26], яка базується на кодових словах ξ_9, ξ_6.

Так, згідно з даними, представленими на рис. 7, при використанні кодових слів ξ_4, ξ_4 у стеганографічному методі з кодовим управлінням вбудовуванням додаткової інформації та сліпим декодуванням під впливом атаки стисненням спостерігається лише на 2,4 % більше помилок у порівнянні з оригінальним стеганографічним методом з кодовим управлінням без сліпого декодування [17] на основі одного з найкращих кодових слів розміру $\mu = 8$, що впливає на трансформанту Уолша – Адамара (5,1).

Стеганографічний метод з кодовим управлінням із сліпим декодуванням характеризується тими самими перевагами, що і класичний варіант стеганографічного методу з кодовим управлінням

вбудовуванням додаткової інформації [17], зокрема, забезпеченням високої надійності сприйняття стеганоповідомлення. Задля оцінки надійності сприйняття стеганоповідомлення загальноприйнятним є показник PSNR (хоча він і не є таким, що вичерпно оцінює надійність сприйняття), який визначається наступним чином:

$$PSNR = 20\lg\left(\frac{255}{\sqrt{MSE}}\right), \tag{30}$$

де показник MSE визначається як

$$MSE = \frac{1}{nm}\sum_i\sum_j \left|X(i,j) - M(i,j)\right|^2. \tag{31}$$

де X – матриця оригінального зображення, M – матриця стеганоповідомлення.

Зважаючи на структуру стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації показник PSNR є стабільним, не залежить від розміру контейнера, залежить лише від застосованого набору кодових слів. Так, встановлено, що у разі застосування в якості t_1 і t_2 однакових кодових слів $\xi_i, \xi_i, i = 1,2,...,16$ всі елементи результуючих кодових слів T_8 є рівними за амплітудою, яка дорівнює 2. При цьому, значення PSNR стеганоповідомлення дорівнює 36,1315 дБ.

У разі, якщо в якості t_1 і t_2 обрано різні кодові слова $\xi_i, \xi_j, i, j = 1,2,...,16, i \neq j$, елементи результуючих кодових слів T_8 є різними за амплітудою, і при цьому максимальна амплітуда даних елементів не перевищує значення 2. При цьому PSNR результуючого стеганоповідомлення дорівнює 42,1524 дБ.

У будь-якому випадку, при застосуванні стеганографічного методу з кодовим управлінням із сліпим декодуванням, вплив на інтенсивність пікселів контейнеру є незначним і суворо контрольованим, що дозволяє домогтися як високих показників PSNR, так і фактично виключити виникнення будь-яких артефактів у результуючих стеганоповідомленнях. Наприклад, на рис. 8 показаний приклад оригінального зображення і стеганоповідомлення, що отримано із застосуванням стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації із сліпим декодуванням

із застосуванням в якості t_1 і t_2 кодових слів ξ_4, ξ_4. При цьому розмір контейнера у форматі JPEG, в який відбувалося вбудовування додаткової інформації склав 1200×1200 пікселів, вбудовування відбувалося у просторі YCbCr у компоненту Y, таким чином обсяг додаткової інформації склав 22 500 біт.

а б

Рисунок 8 – Приклад оригінального зображення (а) і стеганоповідомлення (б), що отримано із застосуванням стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації із сліпим декодуванням

Аналіз даних рис. 8 шляхом суб'єктивного ранжування дозволяє дійти висновку про відсутність видимих спотворень або артефактів на стеганоповідомленні.

1.5. Стеганографічний метод з кодовим управлінням на основі досконалих двійкових решіток

Подальший розвиток концепції стеганографії з кодовим управлінням пов'язаний із необхідністю підвищення пропускної спроможності методів без істотної втрати непомітності та стійкості. У цьому контексті особливий інтерес викликає підхід, який базується на використанні досконалих двійкових решіток – спеціальних

кодових структур, що дозволяють ефективно представляти множину кодових слів із заданими структурними властивостями. На відміну від класичних схем, даний метод орієнтований на вбудовування декількох бітів у межах одного блоку, що істотно розширює пропускну спроможність. При цьому структура досконалих двійкових решіток забезпечує контроль над відстанями між кодовими словами, що сприяє збереженню стійкості до атак і зниженню ймовірності помилкового декодування.

Введемо необхідні визначення.

Визначення 1 [27]. Досконала двійкова решітка – це двовимірна послідовність (матриця):

$$H(N) = \left\| h_{i,j} \right\|, \quad i, j = 0,1,...,N-1, \qquad h_{i,j} \in \{-1,1\}, \tag{32}$$

що має ідеальну двовимірну періодичну автокореляційну функцію (2ПАКФ), елементи якої:

$$R(m,n) = PACF\left(m,n\right) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+n} = \begin{cases} N^2, \text{ для } m = n = 0; \\ 0, \text{ для будь-яких інших } m \text{ і } n, \end{cases} \tag{33}$$

де $m,n = 0,1,...,N-1$, а всі індекси елементів $h_{i+m,j+\tau}$ зведені за модулем N. Наведемо як приклад досконалу двійкову решітку порядку $N = 4$, а також її двовимірну періодичну автокореляційну функцію:

$$A = \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \end{bmatrix},$$

$$R = \begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (34)$$

Твердження 4 [24]. Кожна досконала двійкова решітка порядку N генерує E(N)-клас еквівалентних матриць – досконалих двійкових решіток за допомогою операцій циклічного зсуву по рядкам і стовпцям та інверсій, при цьому потужність класу еквівалентних матриць дорівнює:

$$J_{E(N)} = 2N^2. \quad (35)$$

З дослідження [24] відомо наступне. Якщо задано довільну породжуючу досконалу двійкову решітку $A_0(N)$ порядку N, то всі її циклічні зсуви визначаються як $L_{k_1} A Q_{k_2}$, $k_1, k_2 = 0,1,...,N-1$ і нехай двовимірна періодична взаємнокореляційна функція (2ПВКФ) між $A_0(N)$ та її циклічно зсунутою решіткою визначається співвідношенням:

$$B(m,n) = A_0(N) ** L_{k_1} A_0(N) Q_{k_2} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+\tau}, \quad (36)$$

де символ ** позначає двовимірну кореляцію (згортку); $m, n = 0,1,...,N-1$.

Відоме наступне твердження:

Твердження 5 [24]. 2ПВКФ $B(m,n)$ решітки $A_0(N)$ та решітки $L_{k_1} A_0(N) Q_{k_2}$ порядку N, $k_1, k_2 = 0,1,...,N-1$, є 2ПАКФ $\|R(m,n)\|$ решітки $A_0(N)$, зсунута на k_1 рядків та k_2 стовпців, тобто

$$B(m,n) = R(m+k_1, n+k_2), \quad m,n = 0,1,...,N-1. \quad (37)$$

Запропонований стеганографічний метод базується на принципі модуляції інформації, який використовує ключову властивість досконалих двійкових решіток: 2ПВКФ між досконалою двійковою решіткою та її циклічно зсунутою версією (по рядкам і стовбцям) структурно еквівалентна відповідному циклічному зсуву 2ПАКФ вихідної решітки. Ця алгебраїчна симетрія дозволяє точно та передбачувано маніпулювати піками кореляції. Ми пропонуємо кодувати інформацію, вибираючи один з можливих станів, за допомогою контрольованих циклічних зсувів (або по рядкам, або по стовпцям) у поєднанні з додатковою двійковою інверсією. Таким чином, процес вбудовування відповідає певному перетворенню структури масиву в блоці зображення. Під час вилучення метод спирається на несліпе декодування, типове для схем з кодовим управлінням: реконструюється вбудований компонент, обчислюється 2ПВКФ, і положення її глобального максимуму однозначно визначає біти вбудованого повідомлення.

На відміну від традиційних підходів на основі застосування областей перетворень, запропонований метод працює повністю в просторовій області, використовуючи досконалі двійкові решітки як кодові носії інформації для вбудовування додаткової інформації, що дозволяє здійснювати кодове управління вбудовуванням у частотні складові. Ключова ідея полягає у використанні унікальних характеристик автокореляції та взаємної кореляції досконалих двійкових решіток, зокрема їхньої поведінки при циклічних зсувах та інверсії. Ці алгебраїчні симетрії забезпечують надійне та високопродуктивне кодування даних, зберігаючи при цьому низьку обчислювальну складність та сумісність із ресурсообмеженими середовищами. Далі ми описуємо процедури вбудовування та вилучення, а також схему модуляції, що використовується для представлення інформації за допомогою структурних перетворень досконалих двійкових решіток.

Наведемо основні кроки запропонованого стеганографічного методу на основі [17].

Вбудовування додаткової інформації.

Крок 1. Виконайте стандартне розбиття зображення вихідного контейнера на неперекриваючі блоки розміру $N \times N$.

Крок 2. Виберіть опорну досконалу двійкову решітку $A_0(N)$ розміру N.

Крок 3. Нехай X – наступний блок контейнера, що бере участь у стеганографічному перетворенні. Виберіть вектор $D = \{d_1 \quad d_2 \quad ... \quad d_{\log_2(2N^2)}\}$, який містить наступні $\log_2(2N^2)$ бітів інформації, які будуть вбудовані в цей блок контейнера.

Крок 4. Визначте значення біта d_1 як знак кодування досконалою двійкової решітки, десятковий еквівалент бітів $k_1 = \{d_2 \quad d_3 \quad ... \quad d_{\log_2(N)+1}\}_{10}$ як значення зсуву по рядкам, а десяткових еквівалент бітів $k_2 = \{d_{\log_2(N)+2} \quad d_{\log_2(N)+3} \quad ... \quad d_{\log_2(2N^2)}\}_{10}$ як зсув по стовпцям.

Крок 5. Побудуйте решітку $L_{k_1} A_0(N) Q_{k_2}$ з $E(N)$-класу для вбудовування додаткової інформації та виконайте вбудовування, тоді наступний блок стеганографічного повідомлення буде визначено як

$$M = X + L_{k_1} A_0(N) Q_{k_2}. \tag{38}$$

Зауважте, що при вбудовуванні значення +1 у значення пікселя контейнера 255, а також при вбудовуванні значення −1 у значення пікселя контейнера 0, операція вбудовування для цих пікселів не виконується.

Вилучення додаткової інформації.

Крок 1. Виконайте стандартне розбиття стеганографічного повідомлення на блоки, що не перекриваються розміру $N \times N$.

Крок 2. Нехай $\overline{M}$ – наступний блок можливо збуреного стеганографічного повідомлення, що відповідає блоку X контейнера.

2.1. Побудуйте матрицю $\Delta = \overline{M} - X$ з елементами $\Delta(i, j)$, $i, j = 0,1,...,\mu - 1$, для якого потрібно побудувати матрицю 2ПВКФ:

$$B(m,n) = A_0(N) ** \Delta. \tag{39}$$

2.2. Знайдіть індекси x по рядкам і y по стовпцям максимального (по модулю) значення матриці $B(m,n)$.

2.3. Відновіть вбудовані $\log_2(2N^2)$ біт інформації як

$$\begin{cases} \tilde{d}_1 = sign(B(x,y)) - 1 (\mathrm{mod}\, 3); \\ \{\tilde{d}_2 \quad \tilde{d}_3 \quad ... \quad \tilde{d}_{\log_2(N)+1}\}_{10} = x; \\ \{\tilde{d}_{\log_2(N)+2} \quad \tilde{d}_{\log_2(N)+3} \quad ... \quad \tilde{d}_{\log_2(2N^2)}\}_{10} = y. \end{cases} \tag{40}$$

Ефективність методу оцінюється відповідно до ключових стеганографічних показників, включаючи пропускну спроможність, надійність сприйняття та стійкість до атак проти вбудованого повідомлення. Щоб оцінити ефективність запропонованого методу з точки зору корисного навантаження даних, ми порівнюємо його пропускну спроможність з пропускною спроможністю класичного стеганографічного методу з кодовим управлінням, на основі функцій Уолша – Адамара. Порівняння проводиться для різних розмірів блоків. Тоді як класичний метод зазвичай кодує один біт на блок незалежно від розміру блоку, запропонована схема використовує структурні властивості досконалих двійкових решіток для кодування до $\log_2(2N^2)$ бітів на блок. У табл. 5 підсумовано отримані пропускні спроможності з точки зору кількості бітів на блок та кількості бітів на піксель.

Таблиця 5 – Пропускна спроможність стеганографічних методів

Розмір блоку *N*	**Класичний метод з кодовим управлінням**		**Метод на основі досконалих двійкових решіток**	
	Біт на блок	**Біт на піксель**	**Біт на блок**	**Біт на піксель**
4	1	0,0625	5	0,3125
8	1	0,0156	7	0,1093
16	1	0,0039	9	0,0351

Дані, представлені в табл. 5, демонструють значну перевагу запропонованого методу над класичним методом з кодовим управлінням з точки зору пропускної спроможності. Хоча класичний метод послідовно вбудовує лише 1 біт на блок незалежно від розміру блоку, запропонований метод використовує структурні особливості досконалих двійкових решіток для досягнення значно більшого корисного навантаження. Примітно, що для малих розмірів блоків (наприклад, $N=4$) стеганографічний метод із застосуванням досконалих двійкових решіток має п'ятикратне збільшення пропускної спроможності у вимірі біт на піксель. Навіть для більших блоків, де щільність вбудовування зазвичай зменшується, метод зберігає значну перевагу як у кількості бітів на блок, так і в кількості бітів на піксель. Це підкреслює потенціал методу для застосувань, що потребують високої пропускної спроможності, особливо коли важливо підтримувати візуальну якість. Оцінка точності

сприйняття є складним завданням через суб'єктивну природу людського зорового сприйняття. Зорова система людини демонструє різну чутливість до просторових, частотних та кольорових спотворень, що робить формальну оцінку обмеженою за своєю суттю. Тим не менш, у запропонованому методі модифікація елементів контейнера суворо обмежена: зміни не перевищують за величиною ±1. Це обмеження забезпечує мінімальні спотворення, які, як очікується, будуть непомітними за нормальних умов перегляду. Для підтвердження цього твердження ми надаємо кількісний аналіз з використанням метрики пікового співвідношення сигнал/шум (PSNR) для різних щільностей вбудовування, що відображає частку модифікованих блоків у зображенні.

PSNR оцінюється як

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right), \tag{41}$$

де MSE – це середньоквадратична помилка між оригінальним та зміненим зображенням. Якщо пікселі змінюються на ±1, то

$$MSE = p\frac{1^2}{100} = \frac{p}{100}. \tag{42}$$

У табл. 6 ми наводимо значення PSNR для різних відсотків блоків, що задіяні у стеганоперетвореннi.

Таблиця 6 – Значення PSNR для різних відсотків блоків, що задіяні у стеганоперетворенні

Відсоток блоків, що задіяні у стеганоперетворенні	**MSE**	**PSNR (dB)**
25 %	0,25	54,15
50 %	0,50	51,14
75 %	0,75	49,38
100 %	1,00	48,13

Результати, представлені в табл. 6, підтверджують, що запропонований метод зберігає значну надійність сприйняття за різних відсотків блоків, що приймають участь у стеганоперетворенні. Навіть при 100 % вбудовуванні, де кожен блок бере участь у приховуванні даних, PSNR залишається вище 48 дБ – у межах діапазону, який

вважається візуально непомітним. Ця стійкість випливає з фундаментальної конструкції методу, успадкованої від концепції кодового управління, де модифікації пікселів обмежені значеннями ±1. Завдяки ретельному обмеженню амплітуди змін, запропонований підхід гарантує, що вбудована інформація не вносить помітних візуальних артефактів, таким чином зберігаючи візуальну цілісність зображення.

У табл. 7 ми показуємо отриману залежність коефіцієнта помилок декодування від коефіцієнта стиснення *QF*.

Таблиця 7 – Залежність коефіцієнта помилок при декодуванні від *QF* в умовах атаки стисненням JPEG

QF	100	90	80	70	60
Кількість помилок, %	0,02	26,53	42,88	46,41	47,77
QF	50	40	30	20	10
Кількість помилок, %	48,40	48,88	49,23	49,53	49,82

Експериментальні результати показують, що навіть за відносно невеликого розміру блоку та вбудовування 7 бітів на блок, що представляє семикратне збільшення корисного навантаження порівняно з класичними методами з кодовим управлінням, запропонований метод підтримує прийнятну стійкість за низьких рівнів стиснення JPEG, що є вражаючим результатом, враховуючи поєднання агресивного збільшення пропускної спроможності та стиснення з втратами. Ці результати піднімають важливе та малодосліджене питання в стеганографічному проєктуванні: чи ефективніше використовувати невеликі блоки з обмеженою пропускною спроможністю для забезпечення стійкості, чи використовувати більші блоки, які вміщують більше даних на одиницю?

Як зазначив Шеннон у своїй фундаментальній роботі [28], більші коди часто забезпечують кращу ефективність та стійкість. Екстраполюючи цей принцип, більші розміри блоків потенційно можуть забезпечити підвищену стійкість не лише до артефактів стиснення, але й до стеганалітичних атак через підвищену структурну складність та варіабельність вбудовування. Ця гіпотеза припускає, що традиційна перевага малих одиниць вбудовування в просторовій та трансформаційно-доменній стеганографії, можливо, потребує переоцінки. Отже, це відкриває переконливий напрямок для переосмислення самих

основ стеганографічного проєктування, що може призвести до появи нових принципів та вбудованих архітектур, заснованих на великоблочних алгебраїчних фреймворках.

1.6. Порявніння стеганографічних методів

У табл. 8 проводиться порівняння різних стеганографічних методів на основі концепції кодового управління за такими критеріями: стійкість до атаки стисненням, надійність сприйняття, що визначається показником PSNR, пропускна спроможність R, область вбудовування, можливість сліпого декодування.

Таблиця 8 – Порівняння стеганографічних методів на основі концепції кодового управління із сучасними аналогами

Алгоритм / Метод	% помилок при заданому рівні QF										PSNR, dB	R	Обл, вб,	Сліпе дек,
	10	20	30	40	50	60	70	80	90	100				
Стеганографічний метод з кодовим управлінням [13]														
$T_{(5,1)}$	42,78	29,35	12,21	3,05	0,97	0,72	0,07	0,03	0	0	48,1	1/16	S	–
$T_{(5,4)}$	50	50	49,04	45,56	40,56	29,90	5,60	0,70	0	0	48,1	1/64	S	–
Стеганографічний метод з кодовим управлінням із сліпим декодуванням														
Original [14]	43,09	37,29	33,06	29,66	26,40	22,36	14,48	10,45	7,47	3,89	42,2	1/64	S	+
ξ_4, ξ_4	42,47	37,83	32,96	15,40	4,91	3,32	2,47	1,60	1,23	1,14	36,1	1/64	S	+
ξ_7, ξ_{11}	42,33	36,58	32,35	27,76	22,30	12,48	5,86	4,63	3,09	2,73	42,2	1/64	S	+
Стеганографічний метод з кодовим управлінням на основі досконалих двійкових решіток														
$A_0(N)$	49,8	49,5	49,2	48,9	48,4	47,8	46,4	42,9	26,5	0,02	48,13	7/64	S	–
Сучасні аналоги														
Li, 2021, [6]	–	–	0,02	–	0,02	–	0,01	–	0,01	0,01	~27,1	0,01	NN	+
Wang, 2021, [7]	–	–	0	–	0	–	–	0	–	0	~38,5	0,01	DCT	+
Zhu, 2019, [8]	–	–	–	–	–	–	33,9	7,4	0,3	–	~45	<1/8	DCT	+
Chanu, 2014, [9]	–	–	–	–	23,88	14,1	2,76	0,08	0,08	–	~32,7	1/16	SVD	+
Мельник, 2012, [10]	13	7	5	4	2	2	2	2	2	–	~ 34,7	1/64	SVD	+
Chang, 2007, [11]	–	–	–	–	24,7	14,4	2,71	0,2	0,1	–	~32,7	1/64	SVD	+

У табл. 8 прийняті такі умовні позначення: S – просторова область, DCT – область трансформант ДКП блоків зображення, SVD – область сингулярного розкладання блоків зображення, NN – стеганоперетворення відбувається засобами нейронної мережі.

1.7. Висновки

1. Узагальнено концепцію кодового управління як ефективну основу для побудови сучасних стеганографічних методів, що забезпечують керований вплив на частотні або просторові складові цифрових контейнерів без переходу в частотну область.

2. Формалізовано класичний стеганографічний метод з кодовим управлінням, який характеризується високою надійністю сприйняття стеганоповідомлення, стійкістю до атак стисненням JPEG та незначним впливом на візуальні властивості контейнера.

3. Досліджено варіант методу зі сліпим декодуванням, що дозволяє здійснювати вилучення прихованої інформації без доступу до оригінального контейнера, забезпечуючи при цьому високу точність декодування в умовах атак.

4. Показано обмеження методу сліпого декодування, пов'язані з варіаціями підблоків, і визначено трансформанти Уолша – Адамара, що є оптимальними з погляду компромісу між стійкістю до атак і мінімізацією помилок.

5. Обґрунтовано доцільність використання досконалих двійкових решіток як основи для побудови ефективних кодових конструкцій, які дозволяють підвищити пропускну спроможність стеганографічних методів без втрати стійкості.

6. Проведено комплексне експериментальне оцінювання ефективності різних варіантів кодових слів, що підтвердило можливість адаптації методів до практичних умов – зокрема до атак стиснення, шумових впливів та інших деструктивних дій.

7. Визначено перспективні напрямки подальших досліджень, зокрема розробку багатоканальних кодових конструкцій, побудову метрик взаємного впливу трансформант та створення адаптивних схем вбудовування з урахуванням статистичних властивостей сигналу.

Список використаних джерел

1. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности. Киев : Изд. ГУИКТ. 2009. 251 с.

2. Wang J. et al. The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering.* 2021. Vol. 155. P. 107174.

3. Alaba F. A. The Evolution of the IoT. Internet of Things: A Case Study in Africa. Cham : Springer Nature Switzerland, 2024. P. 1–18.

4. Coiduras-Sanagustín A., Manchado-Pérez E., García-Hernández C. Understanding perspectives for product design on personal data privacy in internet of things (IoT): A systematic literature review (SLR). *Heliyon*. 2024. Vol. 10 (9). P. 1–17.

5. Lam E. Y., Goodman J. W. A mathematical analysis of the DCT coefficient distributions for images. *IEEE transactions on image processing.* 2000. Vol. 9 (10). P. 1661–1666.

6. Li Z., Zhang M., Liu J. Robust image steganography framework based on generative adversarial network. *Journal of Electronic Imaging.* 2021. Vol. 30. Issue 2. P. 023006. doi: 10.1117/1.JEI.30.2.023006

7. Wang S., Zheng N., Xu M. A Compression Resistant Steganography Based on Differential Manchester Code. *Symmetry*. 2021. Vol. 13 (2). P. 345. DOI: 10.3390/sym13020165

8. Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients. *IEEE Access.* 2019. Vol. 7. P. 168613–168628. DOI: 10.1109/access.2019.2953504

9. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. *International Journal of Information & Computation Technology.* 2014. Vol. 4 (7). P. 717–726. DOI: 10.1049/ic:20070706

10. Melnik M. A. Compression-resistant steganographic algorithm. *Information security.* 2012. Vol. 2 (8). P. 99–106.

11. Chang C. C., Lin C. C., Hu Y. S. An SVD oriented watermark embedding scheme with high qualities for the restored images. *International journal of innovative computing, information & control.* 2007. Vol. 3 (3). P. 609–620.

12. Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research

Directions. *IEEE Access.* 2020. Vol. 8. P. 166589–166611. DOI: 10.1109/ACCESS.2020.3022779

13. Bao Z. et al. A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. *Journal of Ambient Intelligence and Humanized Computing.* 2020. Vol. 11 (5). P. 1889–1901. DOI: 10.1007/s12652-019-01345-8

14. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. International Conference on Information Technology in Signal and Image Processing, Mumbai, 2013. P. 416–426.

15. Tao J. et al. Towards robust image steganography. IEEE Transactions on Circuits and Systems for Video Technology. 2018. Vol. 29(2). P. 594–600. DOI: 10.1109/TCSVT.2018.2881118

16. Костирка О. В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования. *Информатика и математические методы в моделировании.* 2013. № 3. С. 275–282.

17. Kobozeva A. A., Sokolov A. V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale*. 2021. Vol. 4 (52). P. 115–130.

18. Kobozeva A. A., Sokolov A. V. Steganographic Method with Code Control of Information Embedding Based on Multi-level Code Words. *Radioelectronics and Communications Systems.* Vol. 66 (4). P. 173–189.

19. Sokolov A. V., Ihnatenko O. O., Balandina N. M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problems of regional energetics.* 2024. Vol. 62 (2). P. 121–137. DOI: 10.52254/1857-0070.2024.2-62.11

20. Sokolov A. V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation.* Vol. 2021. Vol. 11 (3). P. 147–161.

21. Strang G. The discrete cosine transform. SIAM review. 1999. Vol. 41 (1). P. 135–147.

22. Jayathilake A., Perera A. A. I., Chamikara M. A. P. Discrete Walsh-Hadamard transform in signal processing. *IJRIT Int. J. Res. Inf. Technol*. 2013. Vol. 1. P. 80–89.

23. Kobozeva A. A., Sokolov A. V. The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain. *Problemele Energeticii Regionale.* 2022. 54 (2). P. 84–100.

24. Мазурков М. И. Системы широкополосной радиосвязи. Одесса : Наука и Техника, 2010. 340 с.

25. Natural Resources Conservation Service (NRCS), United States Department of Agriculture. URL: https://www.nrcs.usda.gov.

26. Зігінова Ю. К. Модифікований стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації із сліпим декодуванням. *Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії* : міжнародна науково-практична конференція, 01–03 червня 2023 року. С. 68–70.

27. Mazurkov M. I., Chechelnytskyi V. Y., Murr P. Information security method based on perfect binary arrays. *Radioelectronics and Communications Systems.* Vol. 51 (11). P. 612–614. DOI: 10.3103/s0735272708110095

28. C. E. Shannon, A mathematical theory of com-munication. *The Bell system technical journal.* 1948. Vol. 27 (3). P. 379–423.