DOI 10.15276/imms.v15.no4.545
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 4, pp. 545-553

УДОСКОНАЛЕННЯ СТЕГАНОГРАФІЧНОГО МЕТОДУ ВБУДОВУВАННЯ ІНФОРМАЦІЇ В ЧАСТОТНУ ОБЛАСТЬ ЦИФРОВИХ ЗОБРАЖЕНЬ

В. Ю. Волошин, В. В. Подуфалов, Г. Р. Пашнєв, Н. І. Кушніренко

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: 1945vlad1945@gmail.com

На сьогоднішній день існує значна кількість методів та інструментів для приховування інформації у цифрових зображеннях. Проте більшість із них залишаються вразливими до стиснення, фільтрації або інших атак, що призводить до спотворення або втрати прихованих даних. Особливо це стосується методів, які працюють у просторовій області, де навіть незначна обробка зображення може зруйнувати вбудоване повідомлення. Метою роботи є підвищення стійкості та надійності приховування інформації у цифрових зображеннях шляхом удосконалення стеганографічного методу Коха і Жао, який працює в частотній області з використанням дискретного косинусного перетворення (ДКП). У роботі проведено аналіз існуючих стеганографічних методів і програмних засобів, визначено їх переваги та недоліки, що дозволило сформувати напрямок подальшого удосконалення. Розроблений метод включає використання керованого вибору блоків ДКП за допомогою спеціального ключа, що забезпечує рівномірний розподіл прихованих даних і підвищує стійкість методу до JPEG-стиснення. Проведено експериментальні дослідження, які показали покращення показників пікового співвідношення сигналу до шуму (PSNR) у порівнянні з базовим алгоритмом, а також збереження коректності декодування даних навіть після стиснення зображення до 60%. Розроблений метод може бути застосований у системах захисту інформації, цифрового водяного маркування, а також у програмних рішеннях для приховування конфіденційних даних. Отримані результати підтверджують доцільність використання удосконаленого методу Коха і Жао для підвищення надійності та безпеки цифрових зображень. Використання ключового механізму вибору блоків відкриває можливості для побудови більш складних систем багаторівневого приховування інформації. Отримані результати створюють підґрунтя для подальших досліджень у напрямку комбінування стеганографічних і криптографічних методів для забезпечення комплексного захисту цифрових даних.

Ключові слова: стеганографія, метод Коха і Жао, частотна область, цифрове зображення.

Вступ. У сучасному цифровому світі обсяги обміну інформацією невпинно зростають, що підвищує вимоги до захисту даних від несанкціонованого доступу, підробки та перехоплення. Одним із ефективних напрямів забезпечення інформаційної безпеки є стеганографія — метод приховування фактів передавання даних у мультимедійних об’єктах, зокрема у цифрових зображеннях. На відміну від криптографії, стеганографія не лише зберігає конфіденційність повідомлення, але й приховує сам факт його існування, що робить її особливо корисною у сферах безпечного обміну інформацією, цифрового водяного маркування та захисту авторських прав. Попри значний прогрес у розробці стеганографічних методів, багато з них залишаються вразливими до сучасних атак — стиснення JPEG, фільтрації, зміни розміру або конвертації формату. Це особливо стосується методів, що працюють у просторовій області, де навіть незначне редагування зображення може призвести до часткової або повної втрати прихованих даних. Саме тому останніми роками активно розвиваються методи, які використовують частотну область, зокрема на основі дискретного косинусного перетворення. Одним із найбільш відомих і поширених методів частотної стеганографії є метод Коха і Жао, який базується на модифікації коефіцієнтів ДКП. Цей метод характеризується високою

ефективністю, але водночас має обмеження, пов'язані з рівномірністю вибору блоків для вбудовування інформації та зниженням якості зображення при підвищенні стійкості. Уразливість алгоритму до геометричних атак і до втрат при JPEG-стисненні зумовлює необхідність його вдосконалення. З огляду на це, метою даної роботи є удосконалення стеганографічного методу Коха і Жао шляхом запровадження ключового механізму вибору блоків ДКП, що забезпечує більш рівномірний розподіл даних, а також можливість керування параметром вбудовування для досягнення оптимального співвідношення між якістю зображення та стійкістю прихованої інформації. У процесі дослідження було проведено аналіз існуючих методів стеганографії, їх сильних і слабких сторін, а також експериментальне порівняння удосконаленої версії алгоритму з базовим методом. Результати показали, що нова модифікація дозволяє зберегти коректність відновлення даних навіть після суттєвого JPEG-стиснення (до 60%) і забезпечує вищі значення пікового співвідношення сигналу до шуму. Таким чином, розроблений підхід сприяє підвищенню надійності, стійкості та ефективності стеганографічних систем, що підтверджує його актуальність для сучасної кібербезпеки та практичного застосування у сфері захисту цифрової інформації [1].

Мета і задачі роботи. Метою роботи є підвищення стійкості та надійності приховування інформації у цифрових зображеннях шляхом удосконалення стеганографічного методу Коха і Жао з використанням механізму вибору блоків дискретного косинусного перетворення на основі ключа. Для досягнення поставленої мети необхідно розв'язати такі завдання:

- провести аналіз існуючих методів стеганографії, визначити їх переваги та недоліки, а також обґрунтувати вибір методу Коха і Жао як базового;
- дослідити особливості вбудовування інформації в частотну область за допомогою дискретного косинусного перетворення;
- розробити удосконалену модифікацію методу Коха і Жао із використанням ключового механізму вибору блоків для приховування даних;
- провести експериментальні дослідження ефективності запропонованого методу, порівняти його з базовим алгоритмом за показниками якості зображення та стійкості до JPEG-стиснення;

Основна частина. Методи просторової області в стеганографії охоплюють техніки, де приховання даних відбувається безпосередньо в пікселі зображення. Головна мета полягає в тому, щоб ефект наявності повідомлення був непомітним для спостерігача при перегляді зображення. Існують різні способи класифікації методів стеганографії (рис. 1) [2]:

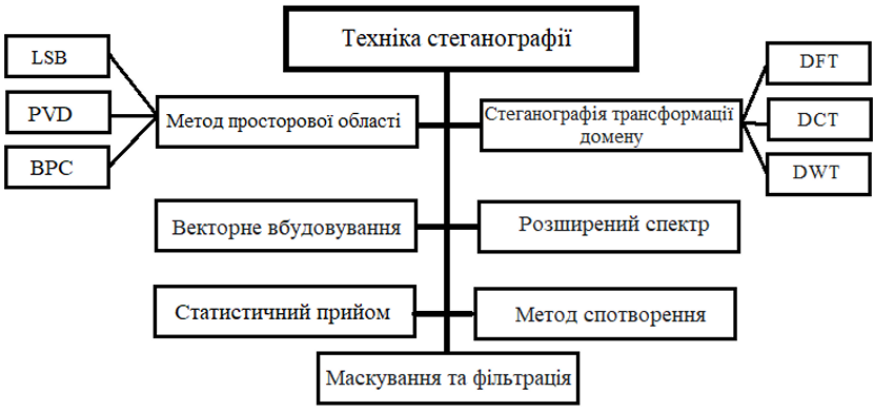

Рис.1. Техніка стеганографії

Дискретне косинусне перетворення (ДКП, DCT) є різновидом лінійного ортогонального перетворення, яке, на відміну від дискретного перетворення Фур'є, забезпечує більш ефективну енергетичну компресію, трансформуючи зображення з

просторової області у частотну, що дозволяє виділити значущі компоненти сигналу для подальшої обробки або стеганографічного вбудовування. Тобто представляє зображення у вигляді матриці 8×8, де зліва зверху знаходяться значення, що відповідають за фонові елементи зображення, а справа знизу – за контури (рис. 2) [3]. Процедура ДКП застосовується до кожного блоку від лівого верхнього кута до правого нижнього кута. Після цього кожен блок стискається з використанням таблиці квантування для масштабування коефіцієнтів ДКП, а потім у стислі блоки вбудовується повідомлення. При необхідності зображення може бути відновлене за допомогою процесу декомпресії, використовуючи зворотне дискретне косинусне перетворення [4].

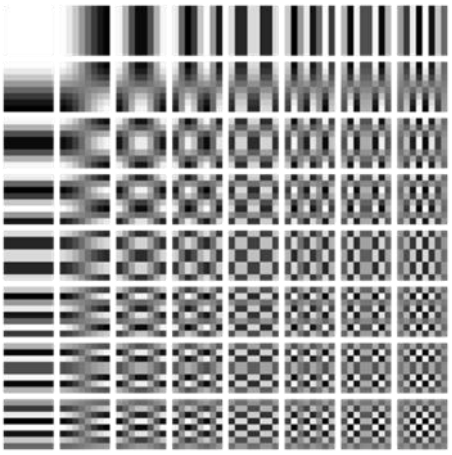

Рис.2. Блок частотної області ДКП

Дискретне косинусне перетворення використовується у JPEG стисненні. Процес стиснення включає в себе обнулення високочастотних складових матриці ДКП, а саме частот, які знаходяться в правому нижньому куті матриці. Ці високочастотні компоненти відповідають за різкі контури і деталі зображення. Тому під час стиснення JPEG саме на контурах можуть з'являтися артефакти, що проявляються у вигляді розмитих областей [5].

ДКП здійснюється за наступною формулою:

$$\mathrm{DCT}(i,j)=\frac{1}{\sqrt{2N}}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}pixel(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right] \qquad (1.1)$$

де j — індекси коефіцієнта DCT у просторі частот;

y — координати пікселя у блоку зображення розміром $N\times N$;

$pixel(x, y)$ — значення інтенсивності пікселя у точці x,y (яскравість);

$C(i)$, $C(j)$ — нормувальні коефіцієнти [6].

Перейдемо до методу Коха і Жао, котрий будемо модифікувати. На початковому етапі первинне зображення стандартним чином розбивається на 8×8 блоки. До кожного блоку, який будемо позначати B, застосовується ДКП, тим самим здійснюючи переведення кожного блоку із просторової в частотну область. У результаті виходить 8×8 блок коефіцієнтів ДКП. Кожний блок призначено для приховання одного біта додаткової інформації (ДІ).

Існує дві реалізації алгоритму:

1. Для вбудови біта ДІ використовуються 2 коефіцієнта ДКП;
2. Для вбудови біта ДІ використовуються 3 коефіцієнта ДКП.

Розглянемо докладно перший варіант. Під час організації прихованого каналу зв'язку абоненти повинні попередньо домовитися (зв'язатися по захищеному каналу зв'язку) про два конкретних коефіцієнта ДКП із кожного блоку, які будуть використовуватися для приховання даних. Задамо дані коефіцієнти їх індексами $u1,v1$ і $u2,v2$ в масивах коефіцієнтів ДКП:

$$\begin{bmatrix} (1,1) & \cdots\cdots & (1,8) \\ \vdots & \cdots\ (u_1,v_1) & \cdots\ \vdots \\ \vdots & \cdots\ (u_2,v_2) & \cdots\ \vdots \\ (8,1) & \cdots\cdots & (8,8) \end{bmatrix}.$$

Відмітимо, що зазначені індекси повинні відповідати середньочастотним коефіцієнтам ДКП, що забезпечить: прихованість інформації; вбудована інформація не буде спотворюватися при Jpeg-стиску зі значними коефіцієнтами якості (або, що те ж саме, з малими коефіцієнтами стиску) [7].

На практиці найчастіше використовуються $u1,v1=4,5$ і $u2,v2=5,4$. Нехай у процесі стеганоперетворення треба вбудувати черговий біт $bk \in 0,1$ ДІ. Відповідно до секретного ключа для цього вибирається блок ЦЗ-контейнера. Відповідний йому блок коефіцієнтів ДКП позначимо $ВДК$:

$$B^{ДКП} = \begin{bmatrix} b_{11}^{ДКП} & b_{12}^{ДКП} & \ldots & b_{18}^{ДКП} \\ b_{21}^{ДКП} & b_{22}^{ДКП} & \ldots & b_{28}^{ДКП} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{81}^{ДКП} & b_{82}^{ДКП} & \ldots & b_{88}^{ДКП} \end{bmatrix}.$$

Для вбудови bk використовуються коефіцієнти $bu1,v1ДКП,$. Вбудова біта bk відбувається таким чином: якщо $bk=0$, то різниця абсолютних значень використовуваних для вбудовування коефіцієнтів ДКП роблять більше деякої заданої додатної величини P, а якщо $bk=1$, то ця різниця робиться менше -P:

$$\begin{cases} \left|b_{u_1,v_1}^{ДКП}\right| - \left|b_{u_2,v_2}^{ДКП}\right| > P, \quad при \quad b_k = 0, \\ \left|b_{u_1,v_1}^{ДКП}\right| - \left|b_{u_2,v_2}^{ДКП}\right| < -P, \quad при \quad b_k = 1. \end{cases}$$

Таким чином, первинне зображення спотворюється за рахунок внесення змін у коефіцієнти ДКП, якщо їх відносні величини не відповідають приховуваному біту. Чим більше P, тим стеганосистема, створена на основі даного методу, є більш стійкою до стиску, однак якість зображення при цьому може значно погіршитися [8].

Після відповідного внесення корекції в значення коефіцієнтів ДКП, проводиться зворотне ДКП блоку. У результаті пересилання стеганоповідомлення, як вже зазначалося вище, зазнає спотворення, спотворення зазнає й ДІ. Для витягу ДІ виконується аналогічна процедура вибору коефіцієнтів ДКП у кожному блоці, що були задіяні в стеганоперетворенні, а розв'язок про переданий біт ухвалюється у відповідності з наступним правилом:

$$\begin{cases} b_k = 0, \quad при \quad \left|\bar{b}_{u_1,v_1}^{ДКП}\right| > \left|\bar{b}_{u_2,v_2}^{ДКП}\right|, \\ b_k = 1, \quad при \quad \left|\bar{b}_{u_1,v_1}^{ДКП}\right| < \left|\bar{b}_{u_2,v_2}^{ДКП}\right| \end{cases},$$

де $bu1,v1ДКП,$ - коефіцієнти ДКП блоку можливо зміненого при передачі стеганоповідомлення [9].

Пропонується додати ключ, за допомогою якого здійснюватиметься вибір блоків дискретного косинусного перетворення, у які буде приховуватися додаткова інформація. Використання ключа дозволить здійснити керований процес вибору блоків, що робить процедуру вбудовування більш організованою та послідовною.

На початковому етапі первинне зображення стандартним чином розбивається на 8×8 блоки однакового розміру. Розбиття виконується за тією ж схемою, що й в оригінальній модифікації методу, що дозволяє забезпечити узгодженість із базовим алгоритмом. Після цього до кожного з отриманих блоків застосовується дискретне косинусне перетворення. Завдяки цьому кожен блок зображення переводиться з просторової області в частотну. У результаті такого перетворення кожен блок зображення представляється у вигляді блоку коефіцієнтів ДКП, які описують його частотні характеристики. Це буде виглядати наступним чином (рис. 3) [10].

U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	U_{16}	U_{17}	U_{18}
U_{21}	U_{22}	U_{23}	U_{24}	U_{25}	U_{26}	U_{27}	U_{28}
U_{31}	U_{32}	U_{33}	U_{34}	U_{35}	U_{36}	U_{37}	U_{38}
U_{41}	U_{42}	U_{43}	U_{44}	U_{45}	U_{46}	U_{47}	U_{48}
U_{51}	U_{52}	U_{53}	U_{54}	U_{55}	U_{56}	U_{57}	U_{58}
U_{61}	U_{62}	U_{63}	U_{64}	U_{65}	U_{66}	U_{67}	U_{68}
U_{71}	U_{72}	U_{73}	U_{74}	U_{75}	U_{76}	U_{77}	U_{78}
U_{81}	U_{82}	U_{83}	U_{84}	U_{85}	U_{86}	U_{87}	U_{88}

Рис.3. Блоки ДКП зі своєю нумерацією

У звичайному методі зазначається, що кожний блок призначений для приховування лише одного біта додаткової інформації. Такий підхід є доволі простим, але він не враховує можливість використання більш гнучкого механізму вибору блоків.

В адаптованому методі пропонується застосувати спеціальний ключ, який буде генеруватися самостійно. Основна вимога до ключа – відсутність повторюваних символів, що забезпечує унікальність та однозначність вибору блоків. Ключ формується у вигляді послідовності з п’яти двозначних чисел, які між собою не повторюються. Для прикладу візьмемо ключ «5312761837». Якщо розділити його на частини, отримаємо п’ять чисел: «53 12 76 18 37». У такому вигляді він зручніше сприймається та дозволяє наочно показати, яким чином відбувається відображення на блоки ДКП. Таким чином, кожне число відповідає конкретному блоку з певною нумерацією, і саме у ці блоки буде приховуватися додаткова інформація. На рисунку 4 подано приклад схематичного відображення вибору блоків відповідно до заданого ключа.

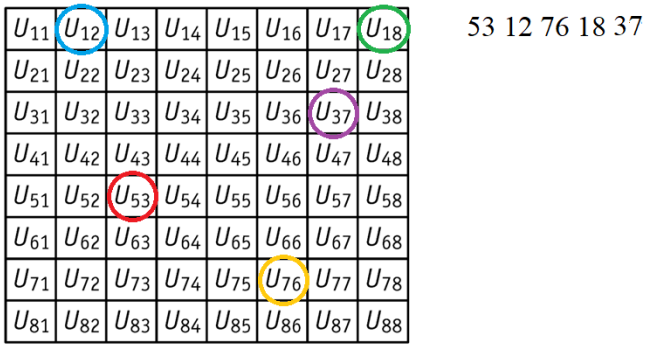

Рис.4. Вбудовування ДІ в ДКП блоки нумерація котрих відповідає ключу

Повторюємо дію для всіх чисел і отримуємо наступний вигляд ДКП блоків, якщо індекси блоків повторюються, то вони просто пропускаються, бачимо наступний рисунок (рис. 5).

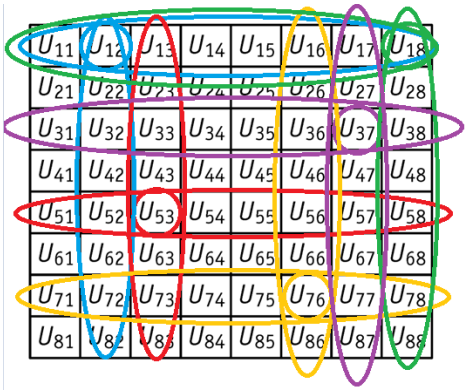

Рис.5. Кінцевий вид блоку в котрий будуть приховані дані

Тобто бачимо що блоки під індексами U21, U24, U25, U41, U44, U45, U61, U64, U65, U81, U84, U85 взагалі не будуть використанні на відміну від оригінального методу в котрому кожний блок призначено для приховання одного біта ДІ.

Далі все відбувається таким самим чином як і в оригінальній модифікації. Окрім того що буде додано можливість обирати значення P, для того щоб користувач сам міг обирати що йому більше потрібно, більший захист чи більша якість.

Експериментальні дослідження проводилися із використанням набору з 100 оригінальних зображень, які мали різний зміст та структуру. У кожне зображення вбудовувалася певна кількість додаткової інформації, виражена у відсотковому співвідношенні до максимально можливої кількості даних, які потенційно можуть бути розміщені у зображенні. Такий підхід дозволив оцінити, як змінюється якість зображень залежно від обсягу прихованої інформації.

У процесі експерименту було проведено серію тестів, під час яких дані вбудовувалися у синій канал зображення. При цьому параметр P було зафіксовано на рівні P = 25. Це дало змогу забезпечити однакові умови для всіх зображень та коректно порівняти результати.

Для оцінювання якості стеганографічних зображень було використано показник пікового співвідношення сигналу до шуму. Отримані значення PSNR дозволяють визначити ступінь спотворення зображення після процесу вбудовування інформації. Чим вищим є значення цього показника, тим менш помітними є зміни для людського ока.

На рисунку 6 зображені результати. Видно, що удосконалена модифікація дає кращі результати від вже наявної.

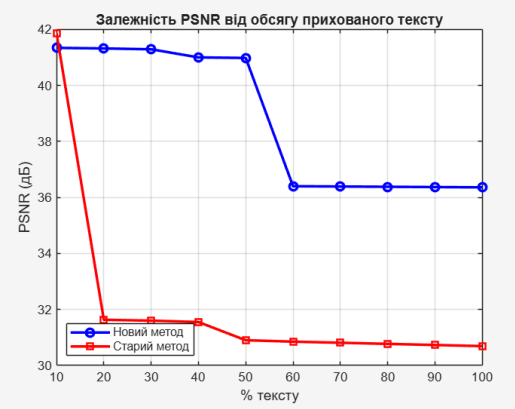

Рис.6. Графік залежності кількості тексту і впливу на PSNR зображення

Для більш ґрунтовної перевірки його можливостей було проведено додатковий експеримент, спрямований на оцінку здатності алгоритму коректно декодувати додаткову інформацію за умов різних рівнів стиснення JPEG.

У даному дослідженні аналізувалася робота методу при змінних значеннях коефіцієнта якості QF, а також при різних параметрах P. Це дозволило оцінити не лише загальну стійкість алгоритму, але й визначити, як саме змінюється його надійність у залежності від умов стиснення.

На рисунку 7 зображені результати. Отримані експериментальні результати підтверджують, що запропонована модифікація демонструє покращені характеристики порівняно з наявним базовим методом. Результати декодування ДІ при значеннях параметра P = 25 та P = 40 не демонструють помітних змін. Однак для значенням P = 55 стало можливим успішно витягти ДІ при стисненні 80%. Подальші експерименти показали, що при значеннях P = 70 та P = 85 цифрову інформацію вдалося відновити за умов стиснення до 70%. Найкращий результат було отримано при P = 100 — навіть за умови стиснення зображення до 60% цифрова інформація була витягнута без спотворень.

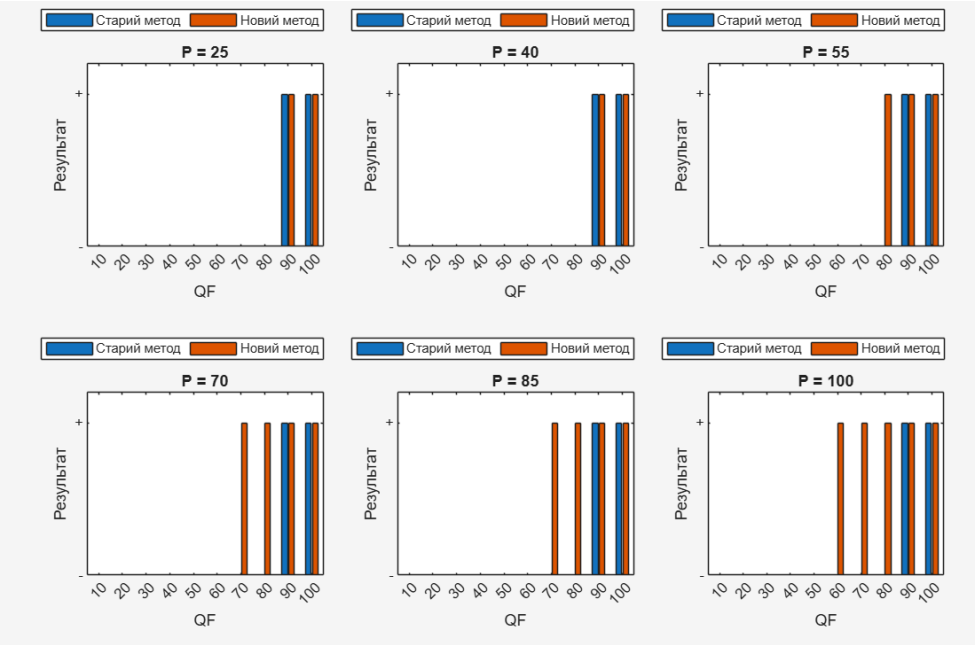

Рис.7. Гістограми можливості декодування ДІ в порівнянні двох методів

Висновки. Проведено дослідження методів стеганографії та їх практичного застосування для приховування інформації у цифрових зображеннях. Було виконано порівняльний аналіз сучасних стеганографічних технік, серед яких особливу увагу приділено методам, що працюють в частотній області. Це дозволило виявити основні недоліки традиційних підходів, зокрема недостатню стійкість до JPEG-стиснення та геометричних атак, що стало підґрунтям для подальшого удосконалення алгоритмів.

У роботі розроблено удосконалену модифікацію методу Коха і Жао, яка базується на використанні ключового механізму вибору блоків дискретного косинусного перетворення. Такий підхід забезпечує рівномірніший розподіл прихованої інформації, зменшує ймовірність спотворень та підвищує стійкість методу до втрат під час стиснення зображень.

Проведено експериментальні дослідження із використанням набору тестових зображень різного типу. За результатами експериментів підтверджено, що удосконалена модифікація демонструє вищі показники пікового співвідношення сигналу до шуму порівняно з базовим методом, а також зберігає можливість коректного декодування додаткової інформації навіть після стиснення зображень до 60% якості.

Розроблений метод відзначається високим рівнем надійності, стійкості та непомітності, що дозволяє рекомендувати його для практичного використання у системах захисту інформації, цифрового водяного маркування та інших задач кібербезпеки, де важливим є збереження якості зображення та безпека переданих даних.

Отже, результати даного дослідження мають як теоретичне, так і практичне значення, оскільки демонструють можливість ефективного удосконалення класичних стеганографічних методів шляхом введення додаткових керованих параметрів та адаптивного вибору блоків в частотній області. Подальші дослідження можуть бути спрямовані на розширення функціональності методу, його інтеграцію з криптографічними механізмами та застосування в системах багаторівневого захисту цифрових медіа.

Список літератури

1. Кулик М.В. Дослідження сучасних алгоритмів побудови цифрових водяних знаків для відео-контенту. Київ: Київський політехнічний інститут імені Ігоря Сікорського. 2018. 40 с.
2. Laskar B., Bouzid M. Enhancing secure communication: a QIM-based steganography approach for G. 722.2 speech streams with Stable Roommate Index Division. *Multimedia Tools and Applications*. 2024. P. 1-19.
3. Agarwal S., Jung K.H. Digital image steganalysis using entropy driven deep neural network. *Journal of Information Security and Applications*. 2024. V. 84. P.103799.
4. Zhang C., Jiang S., Chen Z. SPM: estimating payload locations of QIM-based steganography in low-bit-rate compressed speeches. *Multimedia Tools and Applications*. 2024. P. 1-26.
5. Cohen R. Cryptanalysis of Practical Optical Layer Security Based on Phase Masking of Mode-Locked Lasers and Multi-Homodyne Coherent Detection. *Journal of Lightwave Technology*. 2024.
6. Cohen R. Cryptanalysis of Practical Optical Layer Security Based on Phase Masking of Mode-Locked Lasers. *Journal of Lightwave Technology*. 2023.
7. Нищик В.І. Розробка мобільного додатка для Android з реалізацією методу LSB для стеганографії. Одеса: Одеський державний екологічний університет, 2022. 12 с.
8. Discrete cosine transform. URL: https://www.mathworks.com/help/signal/ref/dct.html
9. Зоріло В.В., Лебедєва О. Ю., Петрук К. О. Виявлення мультиплікативного шуму в цифрових зображеннях в умовах збереження з втратами. Одеса: НУОП, 2023.
10. Dixit M., Bhide N., Khankhoje S., Ukarande R. Video Steganography. *Pervasive Comput*. 2021. V. 1. P. 1–4.

IMPROVEMENT OF A STEGANOGRAPHIC METHOD FOR EMBEDDING INFORMATION INTO THE FREQUENCY DOMAIN OF DIGITAL IMAGES

V. Voloshyn, V. Podufalov, H. Pashniev, N. Kushnirenko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: 1945vlad1945@gmail.com

Today, there are a significant number of methods and tools for hiding information in digital images. However, most of them remain vulnerable to compression, filtering, or other attacks, leading to distortion or loss of hidden data. This is especially true for methods that operate in the spatial domain, where even minor image processing can destroy the embedded message. The aim of this work is to improve the robustness and reliability of information hiding in digital images by improving the steganographic method of Koch and Zhao, which works in the frequency domain using discrete cosine transform (DCT). The paper analyses existing steganographic methods and software tools, identifies their advantages and disadvantages, and suggests directions for further improvement. The developed method involves the use of controlled selection of DCT blocks using a special key, which ensures uniform distribution of hidden data and increases the stability of the method to JPEG compression. Experimental studies have been conducted, which showed an improvement in peak signal-to-noise ratio (PSNR) compared to the baseline algorithm, as well as the preservation of data decoding accuracy even after image compression to 60%. The developed method can be applied in information security systems, digital watermarking, and software solutions for hiding confidential data. The results obtained confirm the feasibility of using the improved Koch and Zhao method to improve the reliability and security of digital images. The use of a key block selection mechanism opens up opportunities for building more complex multi-level information hiding systems. The results obtained provide a basis for further research into combining steganographic and cryptographic methods to ensure comprehensive protection of digital data.
Keywords: steganography, Koch and Zhao method, frequency domain, digital image.