DOI 10.15276/imms.v16.no1.106
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 106-115

ОЦІНКА СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ДЛЯ РІЗНИХ КЛАСІВ КОНТЕЙНЕРІВ

В. В. Кілко, А. В. Соколов

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

Представлено результати експериментального дослідження впливу вибору кодового слова на надійність сприйняття та стійкість стеганографічного вбудовування в зображення. Робота орієнтована на підхід із кодовим управлінням, який дозволяє контролювати процес приховування інформації через параметри кодових структур без зміни області представлення даних. Дослідження виконано на наборі з 500 зображень, класифікованих за рівнем текстурованості (гладкі, середньотекстуровані, високодеталізовані та змішані), що дало змогу встановити закономірності між типом контейнера, вибором кодового слова та відновлюваністю прихованого повідомлення після JPEG-стиску. У межах експерименту розглядалися шість типів кодових слів: постійне (Const), низькочастотне (LF), комбіноване низькочастотне (LF-C), середньочастотне (MF), високочастотне (HF) та Bent. Для кожного зображення здійснювалося вбудовування і подальше відновлення даних після стиску на рівнях якості QF=10…100, а ефективність оцінювалася за показником бітових помилок відновлення. Отримані результати підтвердили, що вибір кодового слова має визначальний вплив на стійкість прихованої інформації, тоді як різниця між класами зображень-контейнерів справляє відчутний, але непорівнянний за масштабом ефект. Встановлено, що низькочастотне кодове слово забезпечує оптимальну стійкість для QF>20, тоді як постійне кодове слово є ефективним при жорсткому стиску (QF≤20). Високочастотне кодове слово доцільно застосовувати лише у сценаріях, де пріоритетом є збереження максимальної візуальної якості, а стійкість не є критичною. Bent кодове слово продемонструвало найменший розкид показників відсотку помилок при вилученні серед усіх класів зображень, підтверджуючи свою універсальність і рівномірний енергетичний розподіл у просторі Уолша-Адамара. Запропоновані рекомендації дозволяють формувати адаптивні системи стеганографії з кодовим управлінням, здатні автоматично підбирати частотний профіль кодового слова відповідно до властивостей контейнера та рівня очікуваного стиску. Отримані результати можуть бути використані для підвищення ефективності й надійності стеганографічних методів у практичних системах.

Ключові слова: стеганографія, JPEG, кодове управління, кодове слово, перетворення Уолша-Адамара, бент-функції, стійкість.

Вступ. У сучасну епоху стрімкого розвитку цифрових технологій частка мультимедійних даних у світовому трафіку постійно зростає. Зображення, аудіо- та відеофайли стали основними носіями інформації в соціальних мережах, засобах масової комунікації, електронній комерції та наукових платформах. Така тенденція відкриває нові можливості для обміну даними, але водночас створює серйозні виклики у сфері інформаційної безпеки.

Одним із найефективніших напрямів захисту інформації в мультимедійних середовищах є стеганографія – наука про приховування факту передавання повідомлення. На відміну від криптографії, що маскує зміст даних, стеганографія дозволяє приховати сам факт їх існування, вбудовуючи секретну інформацію у звичайні медіаоб’єкти. Завдяки цьому вона набуває особливого значення у контексті захисту комунікацій, цифрових прав, а також протидії інформаційним атакам.

Сучасні стеганографічні методи розвиваються в умовах підвищених вимог до їх ефективності. Оцінювання якості таких методів базується на сукупності критеріїв, що визначають практичну придатність алгоритму у реальних умовах використання.

По-перше, важливою характеристикою є надійність сприйняття (perceptual reliability) – здатність стеганоповідомлення зберігати високий рівень візуальної чи акустичної якості після вбудовування додаткової інформації. Будь-які спотворення, помітні для людини чи детектовані автоматизованими засобами контролю якості, можуть свідчити про наявність прихованої інформації та знижують ефективність системи.

Другим критерієм є пропускна здатність (capacity), тобто кількість інформації, яку можливо приховати без порушення надійності сприйняття та стійкості. Висока пропускна здатність забезпечує можливість передавання значних обсягів даних, однак часто супроводжується компромісом із дотриманням інших критеріїв стеганографічної якості.

Третій аспект – стійкість до атак проти вбудованого повідомлення (robustness). У практичних сценаріях мультимедійні файли можуть піддаватися стисненню, фільтрації, перетворенням чи перекодуванню. Ефективний стеганографічний метод повинен гарантувати відновлення прихованого повідомлення навіть після таких спотворень.

Нарешті, не менш важливим критерієм є стійкість до стеганоаналізу (undetectability), тобто здатність алгоритму протидіяти статистичним і машинним методам виявлення факту приховування. Саме цей параметр визначає реальну стійкість стеганосистеми та її здатність забезпечувати непомітний обмін інформацією у ворожому середовищі.

Для більшості сучасних стеганографічних методів досягнення оптимального балансу між надійністю сприйняття, пропускною здатністю та стійкістю до атак проти вбудованого повідомлення забезпечується шляхом використання областей перетворень – таких як дискретне косинусне перетворення (DCT), дискретне вейвлет-перетворення (DWT) або сингулярний розклад (SVD). Робота в цих просторах дозволяє ефективно розподіляти зміни у прихованому носії, зменшуючи візуальні спотворення та підвищуючи стійкість до атак.

Однак такий підхід має низку суттєвих недоліків. Виконання перетворень вимагає значних обчислювальних ресурсів, особливо при роботі з високороздільними мультимедійними об’єктами. Крім того, багаторівнева структура алгоритмів ускладнює реалізацію та аналіз методів, знижує їх швидкодію та створює труднощі під час адаптації до різних форматів даних.

Альтернативним шляхом підвищення ефективності є використання концепції кодового управління (code-based control), яка дозволяє впливати на процес вбудовування не через зміну області представлення даних, а через керування внутрішніми кодовими структурами самого повідомлення. Суть підходу полягає у тому, що вибір кодових слів, їхня комбінація та спосіб розподілу в контейнері можуть визначати, яким саме чином здійснюється вбудовування, забезпечуючи оптимальний компроміс між надійністю сприйняття, стійкістю до атак проти вбудованого повідомлення та пропускною здатністю.

Кодове управління відкриває можливість формування адаптивних стеганографічних систем, у яких поведінка алгоритму визначається не лише параметрами сигналу, а й властивостями кодових конструкцій. Це дозволяє будувати легші, швидші та водночас більш гнучкі методи, які можуть підлаштовуватися під умови середовища або тип загрози без необхідності обчислювано складних переходів до інших просторів.

Проте, існуючі дослідження методів з кодовим управлінням проводилися без урахування особливостей контейнерів. Зазвичай аналіз здійснювався на узагальненій вибірці зображень, без диференціації за їх структурними або статистичними

характеристиками. Такий підхід дозволяє оцінити загальні тенденції, однак не враховує, що властивості окремих зображень можуть істотно впливати на ефективність алгоритму вбудовування.

Особливий інтерес становить питання, як різні контейнери забезпечують стійкість до атак, спрямованих проти прихованого повідомлення, насамперед – до атак стисненням (наприклад, JPEG-компресії). Саме стиснення є однією із найпоширеніших типів впливу на мультимедійні дані, тому воно має вирішальне значення для практичної оцінки надійності стеганографічного методу.

Водночас вплив різних кодових слів на стійкість повідомлення при використанні різних типів контейнерів до цього часу залишається практично недослідженим. Невідомо, чи існують закономірності, які пов'язують структуру контейнера з рівнем збереження вбудованої інформації після атак стисненням, і чи можна цю залежність використати для підвищення ефективності системи кодового управління.

Метою роботи є аналіз впливу різних кодових слів на стійкість стеганографічного методу з кодовим управлінням у контексті використання різних типів зображень-контейнерів.

Дослідження спрямоване на виявлення залежностей між структурними характеристиками кодових слів, властивостями контейнера та рівнем збереження прихованої інформації після дії атак, зокрема – атак стисненням.

Аналіз літературних джерел. У сучасній науковій літературі представлено значну кількість робіт, присвячених дослідженню стеганографії, її методів та підходів до захисту інформації у цифрових носіях. Дослідники зосереджують увагу на різних аспектах цієї проблеми: від розробки алгоритмів вбудовування повідомлень у просторовій області та областях перетворень до комбінованих гібридних схем, інтеграції шифрування, а також застосування глибокого навчання для підвищення надійності сприйняття та інших характеристик методу. У більшості публікацій підкреслюється важливість забезпечення одночасно високої пропускної здатності, надійності відновлення повідомлення та стійкості до атак, однак існує суттєва прогалина у дослідженнях, що диференціюють поведінку алгоритмів залежно від типу контейнера і структури кодових слів. Саме ці аспекти становлять актуальний інтерес для подальшого розвитку стеганографічних методів з кодовим управлінням.

Робота Chinnusami M. та співавторів [1] пропонує гібридну схему IWT+SVD і демонструє, що поєднання цілочисельного вейвлет-перетворення із сингулярним розкладом підвищує надійність сприйняття і стійкість вбудованого зображення в умовах різних шумових моделей; автори також надали GUI для візуальної й кількісної оцінки результатів, що підвищує відтворюваність їхніх експериментів. Водночас у статті відсутній системний розгляд впливу різних класів контейнерів (наприклад, гладкі або високочастотні зображення) на поведінку алгоритму, і питання ролі структури кодових слів у забезпеченні стійкості до конкретних атак (зокрема стисненням) практично не піднімається, через що результати важко екстраполювати на задачу диференціації контейнерів.

Kumar N.N. і співавтори у статті [2] поєднують 2D-SWT з хаотичними техніками для попереднього шифрування перед вбудовуванням, що є корисною ідеєю для підвищення захищеності повідомлення; прототип показує практичність підходу для швидкого дослідження інтегрованих схем шифрування і стеганографії. Однак формат і обсяг роботи обмежують глибину експериментального аналізу: автори використовують невеликі/стандартні набори тестових зображень і базові метрики (PSNR/SSIM), не проводячи дослідження залежності від типів контейнерів або детального аналізу поведінки після різних рівнів стиснення.

Mandal P.C. і співавтори пропонують у [3] основану на IWT схему QVD-LSB з акцентом на високу ємність вбудовування і демонструють ретельні експерименти, що дає міцну технічну основу для методології і показує, як оптимізувати bpp без

катастрофічного погіршення якості. Водночас, як і в багатьох подібних роботах, перевірка виконана на типовому наборі зображень і не включає статистичної класифікації контейнерів за їхніми властивостями, а також не аналізує, як різні конструкції кодових слів (наприклад, різні коди виправлення помилок чи розподілу бітів) впливають на відновлення після стиснення.

Матеріали дослідження Nagini R. V. S. S. S. та співавторів [4] про multi-image стеганографію демонструють перспективність підходу розподілу додаткової інформації між кількома носіями як способу підвищити загальну стійкість і надійність сприйняття, проте практичні експерименти здебільшого виконуються на гомогенних або синтетичних множинах зображень; до того ж застосування DNN/складних стратегій розподілу ускладнює інтерпретацію того, яка саме властивість контейнера (текстура, спектр частот тощо) відповідає за кращу стійкість до стиснення. Через це multi-image підхід дає корисні ідеї для підвищення характеристик стеганографічних методів, але не дозволяє оцінити взаємозалежності типу «структура кодового слова – тип контейнера – відсоток помилок після стиснення».

Систематичний огляд Apau R. та співавторів [5] дає широкий структурований огляд сучасних підходів до протидії статистичному стеганоаналізу, підкреслюючи усталені тренди та методологічні прогалини: зокрема, автори прямо зазначають недостатню різноманітність тестових наборів і брак досліджень, що диференціюють поведінку алгоритмів за типом контейнерів. Це оглядове джерело слугує важливим підґрунтям для формулювання аргументу про недостатність досліджень саме в питанні взаємодії кодових слів і властивостей контейнера при атаках стисненням.

Нарешті, робота Angulakshmi M. й Deepa M. [6] подає ґрунтовний огляд сучасних нейромережевих підходів до стеганографії, включаючи архітектури типу енкодер/декодер та GAN-моделі, які демонструють високу продуктивність і надійність сприйняття. Проте такі методи, попри свої переваги у глибокому приховуванні інформації, залишаються здебільшого «чорними скриньками» з обмеженою інтерпретованістю. Тому для цілей аналітичного дослідження впливу структури кодових слів, закономірностей їх взаємодії з типом контейнера та пошуку контрольованих параметрів вбудовування більш придатними залишаються класичні, добре формалізовані методи (IWT, SVD, QVD-LSB тощо), які забезпечують можливість математичного опису та відтворюваного аналізу.

Новий напрям у стеганографії пов’язаний із використанням методів з кодовим управлінням, які дозволяють керувати процесом вбудовування інформації на рівні окремих кодових слів який був вперше представлений в роботі [7]. В роботі [8] запропоновано стеганографічний метод на основі багаторівневих кодових слів, що забезпечує підвищену стійкість до атак і дозволяє гнучко розподіляти навантаження між різними елементами контейнера, одночасно зберігаючи високу якість зображення. В роботі [9] розширено концепцію на цифрове відео та запропоновано сліпе декодування, що дає змогу відновлювати вбудовану інформацію без доступу до оригінального контейнера, підвищуючи практичну застосовність методу у реальних системах передачі даних. У подальшій роботі [10] детально досліджено ефективність сліпого декодування і показано, що оптимізація структури кодових слів і алгоритму вбудовування дозволяє значно зменшити ймовірність помилок відновлення при різних умовах атак та рівнях стиснення. Ці дослідження окреслюють перспективи розвитку стеганографії нового покоління, де кодове управління виступає ключовим механізмом підвищення стійкості та ефективності вбудовування інформації.

Незважаючи на наявність сучасних робіт, присвячених методам стеганографії з кодовим управлінням та їхню ефективність, у науковій літературі відсутні систематичні дослідження, які б детально аналізували вплив типу контейнера на характеристики таких методів. Зокрема, не розглянуто, як різні властивості зображень чи відео – текстура, спектральні компоненти, частота деталей – взаємодіють із структурою

кодових слів і визначають стійкість до атак, включно з стисненням та іншими поширеними методами втручання. Це створює помітну прогалину, яку актуально заповнити для розуміння реальної ефективності стеганографії з кодовим управлінням у різнорідних цифрових контейнерах.

Опис експерименту. Метою експерименту було з'ясувати, як вибір кодового слова для вбудовування впливає на стійкість прихованої інформації до JPEG-стиску в зображеннях різних типів. Дослідження спрямовувалося на встановлення взаємозв'язку між структурними особливостями зображень, характеристиками кодових слів і точністю відновлення повідомлення після стиску. В експерименті використано 500 зображень формату PNG, розподілених на чотири класи (pic_png1…pic_png4) відповідно до рівня їх текстурованості: гладкі, середньотекстуровані, високодеталізовані та змішані. Така класифікація дала змогу охопити широкий спектр структурних і спектральних характеристик зображень, що є важливим для коректної оцінки впливу вибору кодового слова на стійкість прихованої інформації. Розглядалися шість варіантів вибору кодових слів, які наведені в табл. 1 із відповідним кожному кодовому слову перетворенням Уолша-Адамара: постійна (Const), низькочастотна (LF), низькочастотна комбінована (LF-C), середньочастотна (MF), високочастотна (HF) та Bent. Ці варіанти визначають, які саме коефіцієнти частотної області зазнають модифікації під час вбудовування, формуючи таким чином різні профілі компромісу між надійністю сприйняття стеганоповідомлення та його стійкістю до спотворень, спричинених стиском. Усі кодові слова побудовано на основі функцій Уолша, що забезпечує рівномірний розподіл впливу на задану трансформанту перетворення Уолша-Адамара. Така побудова гарантує контрольоване і збалансоване втручання у структуру зображення. Винятком є бент-кодове слово (Bent), яке сформоване на основі бент-функції – спеціального класу максимально невзаємнокорельованих булевих функцій [11, 12]. Його енергія рівномірно розсіюється по всіх трансформантах простору Уолша-Адамара, створюючи майже ізотропний вплив на частотну область. Саме тому Bent-кодове слово може вважатися еталонним прикладом балансу між хаотичністю та гармонійною рівновагою в частотному представленні.

Для кожного з класу зображень проводилося вбудовування додаткової інформації з використанням послідовно кожного з шести варіантів кодових слів (Const, LF, LF-C, MF, HF та Bent). Кожне зображення-контейнер отримувало однаковий обсяг прихованих даних, що дозволяло порівнювати ефективність різних кодових конструкцій у однакових умовах.

Після вбудовування кожне стеганоповідомлення піддавалося JPEG-стиску з визначеними рівнями якості, що імітувало типові спотворення, до яких можуть потрапляти мультимедійні файли у реальних умовах передачі. Після стиснення проводилося відновлення прихованої інформації, і для кожного експериментального сценарію обчислювався відсоток бітових помилок відновлення.

Таким чином, процедура дозволяла систематично оцінити вплив вибору кодового слова на стійкість прихованої інформації, а також простежити, як тип зображення-контейнера (гладке, середньотекстуроване, високодеталізоване або змішане) модулює ефективність вбудовування та відновлення. Цей підхід забезпечив репрезентативний і контрольований експериментальний майданчик для порівняльного аналізу кодових конструкцій у контексті різних спектральних профілів контейнера.

Таблиця 1

Кодові слова, що брали участь в експерименті і їх перетворення Уолша-Адамара

Кодове слово, що брало участь в експерименті	Перетворення Уолша-Адамара
$Const = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{Const} = \begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$LF = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$	$W_{LF} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$LFC = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{LFC} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$MF = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{MF} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$HF = \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}$	$W_{HF} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 64 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$Bent = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$	$W_{Bent} = \begin{bmatrix} 8 & 8 & 8 & 8 & 8 & 8 & -8 & -8 \\ 8 & -8 & 8 & -8 & 8 & -8 & -8 & 8 \\ 8 & 8 & 8 & 8 & 8 & 8 & -8 & -8 \\ 8 & -8 & 8 & -8 & 8 & -8 & -8 & 8 \\ 8 & 8 & 8 & 8 & 8 & 8 & -8 & -8 \\ 8 & -8 & 8 & -8 & 8 & -8 & -8 & 8 \\ -8 & -8 & -8 & -8 & -8 & -8 & 8 & 8 \\ -8 & 8 & -8 & 8 & -8 & 8 & 8 & -8 \end{bmatrix}$

Результати та обговорення. Далі ми представляємо результати дослідження впливу вибору кодових слів на стійкість стеганоперетворення до JPEG-стиску для різних

класів зображень. Для кожного експериментального сценарію обчислювався відсоток бітових помилок відновлення після стиску. Узагальнені дані за всіма класами зображень та варіантами кодових слів наведені у табл. 2, що дозволяє порівняти ефективність кожної кодової конструкції та простежити закономірності взаємодії між структурними характеристиками контейнера і типом кодового слова.

Таблиця 2.

Відсоток бітових помилок для кожного класу зображень із застосуванням різних кодових слів

Матриця	Група зображень	JPEG Стиск									
		10	20	30	40	50	60	70	80	90	100
Постійна (Const)	pic_png1	40.2	31	22.8	15.9	10.9	7.3	3.9	1	0.3	0.1
	pic_png2	40.3	31.2	23.4	16.9	12	8.5	5	2	0.9	0.4
	pic_png3	40.1	30.6	22.8	16.3	10.9	8	4.9	2.2	1.2	0.7
	pic_png4	40.2	30.8	22.7	16.2	11	7.8	4.8	2	1.1	0.5
Низькочастотна (LF)	pic_png1	42.3	31.4	20.2	11.28	7.2	5	2.8	1.3	0.2	0
	pic_png2	42	31.6	21.3	12.9	8.6	6.4	3.8	2	0.4	0.2
	pic_png3	41.8	30.8	19.6	10	5.7	3.8	1.8	0.8	0.1	0
	pic_png4	42.2	30.8	19.6	10.3	6.1	4.2	1.9	0.9	0.2	0
Низькочастотна комбінована (LF-C)	pic_png1	44.7	36.4	26.5	15.9	9.3	6.7	4.5	2.8	0.8	0
	pic_png2	44.7	36.1	26.8	17.4	10.8	8.2	5.7	3.6	1	0.2
	pic_png3	44.5	35.6	26.2	15.4	7.5	4.9	2.9	1.5	0.3	0
	pic_png4	45.1	36.2	25.9	15.2	7.9	5.3	3.2	1.6	0.4	0
Середньочастотна (MF)	pic_png1	45.6	38	28.2	18.4	8.8	5.9	4.4	3	0.8	0
	pic_png2	45.5	37.6	28.4	20	10.9	7.9	6	4.2	1.3	0.2
	pic_png3	45.3	37.1	27.6	18.8	7.3	4.6	3	1.7	0.4	0
	pic_png4	46	38	27.7	17.8	7.4	4.6	3	1.8	0.5	0
Високочастотна (HF)	pic_png1	49.8	49.6	49.4	49.3	49.2	49	48.6	47.9	43.9	0
	pic_png2	49.8	49.7	49.5	49.3	49.2	48.9	48.4	47.3	41.2	0
	pic_png3	49.8	49.7	49.5	49.3	49.2	48.9	48.6	47.6	42	0
	pic_png4	49.8	49.7	49.5	49.4	49.2	49	48.6	47.7	42	0
Бент (Bent)	pic_png1	46.1	42	37.9	34.3	30.4	26.9	21.4	14.4	4	0
	pic_png2	46.3	42.1	38.2	34.7	31	27.9	22.6	15.4	4.4	0.2
	pic_png3	46.1	41.8	37.9	34.5	30.8	27.4	21.7	13.9	3.1	0
	pic_png4	46.2	41.9	37.9	34.4	31	27.6	22.4	14.9	3.5	0

Аналіз результатів експерименту дозволяє зробити кілька ключових висновків. По-перше, як видно з даних табл. 1.2, зеленим кольором виділені найбільш ефективні кодові слова, які демонструють найнижчий рівень бітових помилок відновлення і можуть бути рекомендовані для практичного використання в системах стеганографії з кодовим управлінням. По-друге, якщо не очікується впливу атак стисненням, доцільно використовувати високочастотне кодове слово, оскільки воно забезпечує максимальну надійність сприйняття контейнера і мінімальні візуальні спотворення, однак його стійкість до JPEG-стиску та інших втручань практично відсутня. По-третє, низькочастотне кодове слово показує високу ефективність при середніх рівнях стиснення до QF=20; для ще більш жорсткого стиску більш доцільним стає застосування кодового слова, що впливає на постійну складову, оскільки воно зберігає відновлюваність бітів навіть у сильно стиснутих зображеннях.

Розподіл ефективності кодових слів також залежить від класу зображень. Для гладких зображень (pic_png1) низько- та середньочастотні кодові слова забезпечують

стабільно низький відсоток помилок, тоді як високочастотні компоненти майже одразу втрачають вбудовану інформацію при стиску. У середньотекстурованих та високодеталізованих зображеннях (pic_png2–pic_png3) перевага кодових слів, що впливають на низькі та середні частоти, менш помітна, проте вони все одно перевершують високочастотні варіанти за стійкістю. Зображення змішаного типу (pic_png4) демонструють проміжні результати, при цьому Bent-кодове слово зберігає передбачуваний рівень відновлення для всіх груп, що свідчить про його універсальність.

Bent-кодове слово, бувши реалізацією максимально невзаємнокорельованих булевих функцій, забезпечує рівномірний розподіл енергії по всіх трансформантах Уолша-Адамара. Завдяки цьому воно демонструє високу стійкість незалежно від спектрального профілю зображення та рівня стиску, поступово знижуючи кількість помилок зі збільшенням коефіцієнта якості JPEG.

Висновки. У роботі проведено системне експериментальне дослідження впливу вибору частотного кодового слова на стійкість стеганографічного вбудовування в зображеннях різних типів. Результати показали, що структура кодового слова істотно впливає на бітову похибку відновлення після стиску, а характер залежності змінюється залежно від класу зображення. Вплив типу контейнера на стійкість також виявлено, однак він є відчутно меншим порівняно з ефектом вибору кодового слова:

1. Встановлено, що низькочастотне кодове слово забезпечує найкращий баланс між надійністю сприйняття та стійкістю для зображень при рівнях якості JPEG QF > 20. Для жорстких умов стиску (QF ≤ 20) ефективнішим є кодове слово, що впливає на постійну складову (Const), оскільки воно дозволяє зберігати відновлюваність прихованих даних навіть у сильно стиснутих контейнерах.

2. Для сценаріїв, де стійкість до атак не є критичною, доцільно використовувати високочастотне кодове слово, що забезпечує мінімальні візуальні спотворення контейнера та високу надійність сприйняття.

3. Bent-кодове слово продемонструвало стабільні результати для всіх типів зображень і рівнів стиску, причому розкид відсотків помилок виявився найменшим. Це підтверджує універсальний характер його спектрального розподілу та можливість використання Bent-кодових слів як еталонних або контрольних конструкцій у системах стеганографії з кодовим управлінням.

4. У цілому можна стверджувати, що вибір кодового слова слід здійснювати адаптивно:

- для QF > 20 – перевага низькочастотних кодових слів;
- для QF ≤ 20 – постійне кодове слово;
- якщо важливою є незалежність стійкості стеганоповідомлення від класу контейнера – Bent кодове слово демонструє такі властивості.

Отримані результати формують основу для подальшої розробки адаптивних стеганографічних систем з кодовим управлінням, де вибір частотного профілю кодового слова може автоматично підлаштовуватися під спектральні властивості контейнера та очікуваний рівень стиску.

Список літератури

1. Chinnusami M. Analysis of hybrid integer wavelet transform and singular value decomposition for image steganography under various noise conditions. *Scientific Reports*. 2025. Vol. 15, No. 1. P. 31610. DOI: 10.1038/s41598-025-17020-2
2. Kumar N. N., Viswanathan R., Kumar P. S. An Efficient Approach on Image Encryption Steganography based on 2D SWT with Chaotic Techniques. *4th International Conference on Soft Computing for Security Applications. IEEE*. 2024. P. 479-486. DOI: 10.1109/icscsa64454.2024.00083

3. Mandal P.C., Mukherjee I., Chatterji B.N. Integer wavelet transform based high performance secure steganography scheme QVD-LSB. *Multimedia Tools and Applications.* 2024. Vol. 83, No. 23. P. 62651-62675. DOI:10.1007/s11042-023-17927-w
4. Nagini R.V. Advancing communication security through multi-image steganography. AIP Conference Proceedings. *AIP Publishing LLC.* 2025. Vol. 3263, No. 1. P. 150001. DOI: 10.1063/5.0261581
5. Apau R. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PloS one.* 2024. Vol. 19, No. 9. P. e0308807. DOI: 10.1371/journal.pone.0308807
6. Angulakshmi M., Deepa M. Image Stenography Using Deep Learning Techniques. Enhancing Steganography Through Deep Learning Approaches. *IGI Global.* 2025. P. 53-74. DOI: 10.4018/979-8-3693-2223-9.ch003
7. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale.* 2021. No. 4 (52). P. 115-130. DOI:: 10.52254/1857-0070.2021.4-52.11
8. Кобозєва А.А., Соколов А.В. Стеганографічний метод з кодовим управлінням вбудовуванням інформації на основі багаторівневих кодових слів. *Вісті вищих учбових закладів. Радіоелектроніка.* 2023. Т. 66, №4. С. 205-222. DOI: 10.20535/s0021347023040052
9. Кілко В.В., Соколов А.В., Баландіна Н.М. Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео. *Кібербезпека та комп'ютерно-інтегровані технології.* 2024. С. 110-114.
10. 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, No. 2. P. 121-137. DOI: 10.52254/1857-0070.2024.2-62.11
11. Rothaus O. S. On "bent" functions. *Journal of Combinatorial Theory, Series A.* 1976. Vol. 20, No. 3. P. 300-305. DOI: 10.1016/0097-3165(76)90024-8
12. Sokolov A.V., Tsevukh I.V. Construction Method for Infinite Families of Bent Sequences. *Journal of Telecommunication, Electronic and Computer Engineering.* 2018. Vol. 10, No. 2. P. 51-54.

ASSESSMENT OF THE ROBUSTNESS OF A STEGANOGRAPHIC METHOD WITH CODE-BASED CONTROL FOR DIFFERENT CLASSES OF CONTAINERS

Kilko V.V., Sokolov A.V.

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine

The paper presents the results of experimental research on the influence of the choice of codeword on the reliability of perception and robustness of steganographic embedding in images. The paper focuses on an approach with code control, which enables the control of information hiding through code structure parameters without altering the data representation domain. The research was conducted on a set of 500 images classified by texture level (smooth, medium-textured, highly detailed, and mixed), which enabled the establishment of patterns between the type of container, the choice of codeword, and the recoverability of the hidden message after JPEG compression. Six types of codewords were considered in the experiment: constant (Const), low-frequency (LF), combined low-frequency (LF-C), medium-frequency (MF), high-frequency (HF), and Bent. For each image, embedding and subsequent recovery of data after compression were performed at quality levels QF=10…100, and the efficiency was evaluated by the recovery bit error rate. The results confirmed that the choice of codeword has a decisive influence on the stability of the hidden information, while the difference between the classes of container images has a noticeable but incomparable effect in scale. It was found that the low-frequency codeword provides the optimal robustness for QF>20, while the constant codeword is effective for hard compression (QF≤20). The high-frequency codeword is advisable to use only in scenarios where the priority is to preserve maximum reliability of perception, and robustness is not critical. The bent codeword demonstrated the smallest spread in the percentage of errors during extraction among all image classes, confirming its universality and uniform energy distribution in the Walsh-Hadamard domain. The proposed recommendations allow the formation of adaptive steganography systems with code control, capable of automatically selecting the frequency profile of the codeword according to the properties of the container and the level of expected compression. The results obtained can be used to improve the efficiency and reliability of steganographic methods in practical systems.

Keywords: steganography, JPEG, code control, codeword, Walsh-Hadamard transform, bent functions, robustness.