

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інформаційних технологій та інноваційного
підприємництва

Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних завдань з дисципліни

«СТЕГАНОГРАФІЯ ТА СТЕГАНОАНАЛІЗ»

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор,
завідувачка кафедри «Кібербезпека та захист інформації»

Методичні вказівки схвалено на засіданні кафедри «Кібербезпека та захист
інформації»

(Протокол від «06» жовтня 2025 р. № 2)

Методичні вказівки схвалено на засіданні НМК ННІ ІТІП

(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

ВСТУП	4
ПРАКТИЧНЕ ЗАВДАННЯ №1. Дослідження властивостей методу модифікації найменшого значущого біта, що виконує стеганоперетворення у просторовій області цифрового контенту	5
ПРАКТИЧНЕ ЗАВДАННЯ №2. Дослідження властивостей методу Коха і Жао, що виконує стеганоперетворення у частотній області цифрового контенту	14
ПРАКТИЧНЕ ЗАВДАННЯ №3. Стеганоаналіз методу модифікації найменшого значущого біта, що виконує стеганоперетворення у просторовій області цифрового контенту	22
ПРАКТИЧНЕ ЗАВДАННЯ №4. Дослідження можливостей виявлення наявності додаткової інформації в цифровому зображенні, вбудованої методом Коха і Жао	26
Література	28

ВСТУП

У сучасних умовах цифрової трансформації суспільства та стрімкого розвитку інфокомунікаційних технологій традиційні методи захисту інформації, що базуються на відкритому шифруванні, часто виявляються недостатніми. Сам факт застосування криптографії привертає увагу зловмисників, роблячи їх об'єктом цілеспрямованих атак, блокування чи глибокого інспектування трафіку. У зв'язку з цим критично важливим напрямом сучасних досліджень і практичної інженерії захисту даних стає комп'ютерна стеганографія та стеганоаналіз - галузь, що забезпечує приховану передачу конфіденційних повідомлень всередині легітимних мультимедійних контейнерів (цифрових зображень, аудіо- та відеопотоків) без виявлення самого факту такої передачі.

Вибіркова дисципліна «Стеганографія та стеганоаналіз» посідає ключове місце у професійній підготовці здобувачів вищої освіти магістерського рівня за спеціальністю F5 Кібербезпека та захист інформації. Магістр з кібербезпеки повинен розуміти архітектурні принципи побудови прихованих каналів зв'язку, механізми вбудовування даних у просторово-частотній області та методи виявлення таких слідів (стеганоаналіз). Це дозволяє ефективно протидіяти внутрішнім загрозам, несанкціонованому витоку корпоративних чи державних даних через мультимедійні канали.

У межах дисципліни магістранти вчаться не просто використовувати готові програмні реалізації, а критично аналізувати стійкість алгоритмів до атак. Це пряма підготовка до професійного аудиту безпеки та виявлення прихованих уразливостей у складних інформаційних системах.

Практичні завдання та методологічні підходи, що опановуються під час вивчення дисципліни, формують міцну базу для виконання кваліфікаційної магістерської роботи. Здобувачі набувають навичок постановки наукових завдань, проведення експериментального моделювання та оцінки ефективності алгоритмів захисту інформації.

Методичні вказівки покликані допомогти магістрантам систематизувати теоретичні знання, закріпити їх на практиці, а також підготувати їх до самостійної вирішення складних завдань забезпечення кіберзахисту в реальному середовищі.

ПРАКТИЧНЕ ЗАВДАННЯ №1

Тема: ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ МЕТОДУ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА, ЩО ВИКОНУЄ СТЕГАНОПЕРЕТВОРЕННЯ У ПРОСТОРОВІЙ ОБЛАСТІ ЦИФРОВОГО КОНТЕНТУ

Мета: Дослідити вплив параметрів LSB-вбудовування на статистичні, візуальні, характеристики матриці цифрового зображення-стеганоповідомлення, а також характеристики його чутливості.

Практичне завдання №1 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Теоретичні відомості

Цифрове зображення в градаціях сірого у комп'ютерній пам'яті представляється у вигляді матриці яскравостей пікселів, де кожен елемент зазвичай займає 1 байт (8 біт) і приймає значення від 0 (чорний) до 255 (білий). У кольорових зображеннях (схема RGB) кожен піксель складається з трьох таких байтів - по одному на червоний, зелений та синій канали. Оскільки кожен байт - це двійкове число, його можна розглядати як суму степенів двійки, де кожен розряд має свою «вагу». Найстарший біт визначає основну яскравість, тоді як наймолодший біт (або найменший значущий біт) (LSB – *Least Significant Bit*) відповідає за найменшу зміну інтенсивності кольору.

Суть стеганографічного методу модифікації найменшого значущого біта – LSB-методу полягає в заміні наймолодшого біта в байті, що визначає яскравість чергового пікселя, контейнера бітом секретного повідомлення. Вбудова біта додаткової інформації призводить до зміни яскравості пікселя лише на ± 1 , або взагалі залишає її незмінною. Для системи людського зору така зміна є нижчою за поріг чутливості ока. Таким чином, вбудована інформація візуально розчиняється в природному шумі зображення, не створюючи видимих артефактів.

Математично процес вбудовування одного біта b у піксель P можна описати наступним чином:

$$\bar{P} = P - (P \bmod 2) + b$$

де $\bar{P}$ - значення пікселя після стеганоперетворення. Операція $P - (P \bmod 2)$ віднімання від первісного значення яскравості залишку від ділення цього

значення на 2 фактично обнуляє молодший біт пікселя-оригіналу, після чого до нього додається біт даних.

Умовно можна вважати, що процес вбудовування додаткової інформації складається з трьох етапів:

- Спочатку секретне повідомлення перетворюється у послідовний потік бітів в результаті роботи прекодера стеганографічної системи;
- Обирається підмножина пікселів контейнера (послідовно, за псевдовипадковим законом чи інакше) для вбудови додаткової інформації, тобто формується стеганошлях, який, як правило, є частиною секретного ключа стеганосистеми;
- Біти повідомлення замінюють оригінальні найменш значущі біти пікселів, що належать стеганошляху.

Якщо при вбудові додаткової інформації використовуються всі пікселі ЦЗ-контейнера, то пропускна спроможність прихованого каналу зв'язку тут становитиме 1 біт/піксель для ЦЗ в градаціях сірого, і 3 біт/піксель – для кольорового (схема RGB), не призводячи до появи артефактів на ЦЗ-стеганоповідомленні. Таку потенційно можливу пропускну спроможність не забезпечує жоден з сучасних стеганографічних методів. Але використання LSB-методу в умовах значної пропускну спроможності призводить до його нестійкості до виявлення: існує велика кількість ефективних стеганоаналітичних методів, що легко виявляють тут наявність вбудованої додаткової інформації, тому на сьогодні дуже часто LSB-метод застосовується в умовах незначної пропускну спроможності прихованого каналу.

Вилучення додаткової інформації відбувається за зворотним алгоритмом і не потребує наявності оригінального зображення-контейнера. Отримувач проходить по стеганошляху і зчитує значення найменших значущих бітів значень яскравості відповідних пікселів. Головною умовою успішного декодування додаткової інформації є синхронізація: отримувач повинен знати точний порядок обходу пікселів - стеганошлях.

Хоча класичний LSB-підхід обмежується заміною лише одного наймолодшого біта, теоретично та практично ніщо не заважає використовувати декілька (k) молодших розрядів (k -LSB, де $k > 1$). У такому разі пропускна спроможність прихованого каналу зростає лінійно: при $k=2$ ми отримуємо 2 біт/піксель для монохромного зображення або 6 біт/піксель для кольорового RGB-зображення, що дозволяє приховати вдвічі більше даних. Проте такий підхід є ризикованим: кожне збільшення k збільшує амплітуду потенційного спотворення значення яскравості пікселя контейнера, що може стати помітним навіть неозброєним оком, особливо на рівномірних ділянках зображення. Вибір оптимального значення k є типовою задачею оптимізації.

Взагалі концепція LSB не обмежена виключно просторовою областю ЦЗ (пікселями). Її можна ефективно застосовувати до будь-яких цифрових коефіцієнтів, що отримані в результаті математичних перетворень. Найпоширенішим прикладом є вбудовування в область дискретного косинусного перетворення (DCT), яке лежить в основі формату JPEG. У цьому випадку біти повідомлення замінюють найменші значущі біти квантованих коефіцієнтів частот. Хоча візуально такі зміни ще важче відстежити, оскільки

вони «розчиняються» у частотному спектрі зображення, це залишає систему надзвичайно чутливою до збереження стеганоповідомлення з втратами.

Аналогічно метод LSB успішно інтегрується у вейвлет-перетворення (DWT). Тут вбудовування відбувається у коефіцієнти деталізуючих піддіапазонів (вертикальних, горизонтальних або діагональних). Це дозволяє реалізувати більш складну стратегію захисту: наприклад, використовувати молодші біти лише тих коефіцієнтів, які відповідають текстурним областям зображення.

Метод LSB знаходить застосування навіть у матричних розкладах, таких як сингулярний розклад (SVD). Вбудовування може здійснюватися в найменші значущі біти округлених до цілих значень сингулярних чисел.

Варто також зауважити, що LSB-підхід не є прерогативою лише статичних зображень. Він є базовим для приховування даних у цифровому аудіо (формати WAV, PCM), де молодші біти відліків амплітуди звукової хвилі замінюються секретною інформацією. В аудіостеганографії це створює ефект легкого фонового шипіння, яке людське вухо часто ігнорує. Також метод активно використовується у відеопотоках, де дані можуть розподілятися між кадрами, що значно підвищує загальну пропускну спроможність прихованого каналу зв'язку.

Таким чином, LSB - це універсальна концепція «найменшого збурення». Незалежно від того, в якій області відбувається стеганоперетворення (просторовій, області перетворення), ми працюємо з межею між інформативним сигналом та неминучим цифровим шумом. Вміння маніпулювати цією межею, не порушуючи статистичної рівноваги системи, і є головним завданням сучасної інтелектуальної стеганографії.

Переваги та недоліки методу модифікації найменшого значущого біта

Переваги методу LSB:

1. Висока потенційно можлива пропускну спроможність прихованого каналу зв'язку;
2. Висока візуальна якість отриманого стеганоповідомлення;
3. Порівняно низька обчислювальна складність: $O(n)$ операцій при використанні n пікселів ЦЗ-контейнера. LSB-метод не потребує складних математичних перетворень, є простим в практичній реалізації, що дозволяє використовувати його в режимі реального часу на малопотужних пристроях.
4. Для отримання секретного повідомлення не потрібно мати оригінальний контейнер. Достатньо знати стеганошлях, що використовувався при вбудові додаткової інформації, що є частиною секретного ключа.

Недоліки методу LSB:

1. Нестійкість до будь-якої атак проти вбудованого повідомлення: будь-яке незначне збурення матриці стеганоповідомлення - зміна розміру, незначний поворот, фільтрація, накладання шуму, розмиття, стиск з втратами руйнує вбудовану додаткову інформацію. При цьому кількісною оцінкою ефективності декодування виступає коефіцієнт кореляції NC між вбудованою додатковою інформацією

$p_1, p_2, \dots, p_t, \bar{p}_i \in \{0,1\}$, $i = \overline{1, t}$, що є результатом попереднього кодування секретного повідомлення, і декодованою $\bar{p}_1, \bar{p}_2, \dots, \bar{p}_t, \bar{p}_i \in \{0,1\}$, $i = \overline{1, t}$:

$$NC = \sum_{i=1}^t p_i' \times \bar{p}_i' / t, \quad (1.1)$$

де $p_i' = 1, \bar{p}_i' = 1$, якщо $p_i = 1, \bar{p}_i = 1$, і $p_i' = -1, \bar{p}_i' = -1$, якщо $p_i = 0, \bar{p}_i = 0$.
Чим менше NC , тим більшим є ступінь чутливості стеганоповідомлення.

2. При значній пропускній спроможності прихованого каналу (>0.25 біт/піксель) LSB-метод є вкрай нестійким до стеганоаналізу.

Варіанти практичного завдання №1

Кожен варіант розрахований на команду з двох студентів: студент А, студент Б.

Варіант 1: Дослідження k -LSB-методу в просторовій області та стратегій розподілу збурень в сенсі забезпечення надійності сприйняття формованого стеганоповідомлення.

1. Задача дослідження

Головна задача при організації прихованого (стеганографічного) каналу зв'язку – забезпечення надійності сприйняття стеганоповідомлення.

При фіксованому секретному повідомленні (бінарній послідовності, що є результатом роботи прекодера стеганосистеми) довжиною M біт є два шляхи:

1. Використання 1-LSB-методу, тобто задіяти M пікселів ЦЗ-контейнера, змінивши в кожному лише 1 найменший значущий біт.
2. Використання k -LSB-методу, тобто задіяти M/k пікселів, змінивши в кожному k молодших бітів.

Дослідити візуальну якість формованого стеганоповідомлення: залежність візуальної якості від k для ЦЗ-контейнерів, що мають різні властивості; вплив характеристик ЦЗ на значення k , при якому починають виникати артефакти на ЦЗ-стеганоповідомленні.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Сформувані секретне повідомлення – бінарну послідовність довжини M біт.

2.3. Вбудувати повідомлення методом k -LSB в кожний з контейнерів, де $k \in \{1, 2, 3, 4, 5, 6\}$, обираючи стеганошлях випадковим чином.

2.4. Для кожного стеганоповідомлення розрахувати показник візуального спотворення PSNR (Peak Signal-to-Noise Ratio). Побудувати графік залежності значення PSNR від k .

2.5. Оцінити візуальну якість всіх отриманих стеганоповідомлень шляхом суб'єктивного ранжування (враховуючи думку всіх зацікавлених сторін).

Порівняти суб'єктивну і кількісну оцінку візуальної якості. Занести ваші результати у відповідну таблицю.

Оцінка візуальної якості ЦЗ з папки «А»		Оцінка візуальної якості ЦЗ з папки «Б»	
PSNR	Шляхом суб'єктивного ранжування	PSNR	Шляхом суб'єктивного ранжування

Пояснити отримані результати.

2.6. Визначити таке значення k , при якому починають виникати артефакти на ЦЗ-стеганоповідомленні. Чи однаковим буде це значення для ЦЗ з папок «А», «Б»? Пояснити отримані результати.

2.7. Побудувати гістограми значень яскравості поданих контейнерів і відповідних їм стеганоповідомлень. Пояснити властивості отриманих гістограм.

2.8. Сформулювати висновки, рекомендації по використанню контейнерів, k -LSB-методу по результатах проведеного дослідження.

Контрольні запитання:

1. Чому PSNR може бути однаковим для 1-LSB-методу та k -LSB, але візуальна якість буде різною?
2. Уявіть, що при передачі стеганоповідомлення у каналі зв'язку стався збій, і один піксель стеганоповідомлення був спотворений. Поясніть, як значення k в k -LSB-методі вплине на показник похибки при декодуванні додаткової інформації.
3. Який з k -LSB-методів будете використовувати за необхідності Ви? Поясніть свою відповідь.

Варіант 2: Дослідження впливу використовуваної для вбудови додаткової інформації колірної компоненти кольорового зображення на візуальну якість отриманого стеганоповідомлення.

1. Задача дослідження

Головна задача при організації прихованого (стеганографічного) каналу зв'язку – забезпечення надійності сприйняття стеганоповідомлення.

Дослідити, чи можна виокремити таку колірну складову кольорового зображення, яка є найбільш придатною для вбудови додаткової інформації з точки зору забезпечення візуальної якості отриманого стеганоповідомлення; як відіб'ється перехід цифрового кольорового зображення з схеми збереження RGB у YCbCr на властивостях отриманого стеганоповідомлення.

2. Завдання

2.1. Обрати кольорові ЦЗ-контейнери: студент А з папки «А»; студент Б з папки «Б».

2.2. Сформулювати секретне повідомлення – бінарну послідовність довжини M біт.

2.3. Розкласти RGB-зображення на три окремі матриці – колірні компоненти: R, G, B.

2.4. Вбудувати сформовану на кроці 2.2 бінарну послідовність методом модифікації найменшого значущого біта по чергово:

- Тільки в канал «Red»;
- Тільки в канал «Green»;
- Тільки в канал «Blue».

В кожному разі зібрати зображення-стеганоповідомлення відповідно зі схемою RGB і розрахувати показник візуального спотворення стеганоповідомлення відносно первісного контейнера.

2.5. Виконати перетворення поданих контейнерів зі схеми збереження RGB у схему YCbCr, використовуючи:

$$\begin{aligned}Y &= 0.299R + 0.587G + 0.114B; \\Cb &= 128 - 0.168R - 0.331G + 0.5B; \\Cr &= 128 + 0.5R - 0.418G - 0.081B.\end{aligned}$$

Вбудувати сформовану на кроці 2.2 бінарну послідовність методом модифікації найменшого значущого біта в канал Y (яскравість) та окремо в канал Cb (синя колірність).

2.6. Виконати зворотне перетворення отриманої стеганоповідомлення в схему RGB для візуалізації результату стеганоперетворення:

$$\begin{aligned}R &= Y + 1.402 (Cr - 128); \\G &= Y - 0.344136 (Cb - 128) - 0.714136 (Cr - 128); \\B &= Y + 1.772 (Cb - 128).\end{aligned}$$

2.7. Обчислити значення пікового відношення «сигнал-шум» PSNR для всіх 5 випадків (R, G, B, Y, Cb) всіх ЦЗ контейнерів.

2.8. Оцінити візуальну якість всіх отриманих стеганоповідомлень шляхом суб'єктивного ранжування. Порівняти суб'єктивну і кількісну оцінку візуальної якості. Занести ваші результати у відповідну таблицю.

Оцінка візуальної якості ЦЗ з папки «А»		Оцінка візуальної якості ЦЗ з папки «Б»	
PSNR	Шляхом суб'єктивного ранжування	PSNR	Шляхом суб'єктивного ранжування

Проаналізувати отримані результати.

2.9. Виокремити таку колірну складову кольорового зображення, яка є найбільш придатною для вбудови додаткової інформації з точки зору забезпечення візуальної якості отриманого стеганоповідомлення. Поясніть свій висновок. Чи залежить Ваш висновок від того, які ЦЗ ви обирали як контейнери (папки «А», «Б»)

2.10. На основі проведеного дослідження надати рекомендації по використанню кольорових ЦЗ в якості контейнерів різних схемах збереження (RGB, YCbCr).

Контрольні запитання:

1. Поясніть, чому для різних каналів значення PSNR може співпадати при вбудові одної додаткової інформації, а візуальне сприйняття результуючого кольорового стеганоповідомлення може бути різним.
2. Чи можна стверджувати, що канал Y в схемі YCbCr є більш прихований, в порівнянні з кожним з каналів R, G, B в схемі RGB? Відповідь пояснити.
3. Як в якості контейнера саме Ви будете використовувати кольорове ЦЗ? Відповідь пояснити.

Варіант 3: Дослідження стійкості до атак проти вбудованого повідомлення k -LSB-методу в просторовій області.

1. Задача дослідження

Дослідити залежність стійкості до атак проти вбудованого повідомлення k -LSB-методу від k для ЦЗ-контейнерів, що мають різні властивості.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Сформувати секретне повідомлення – бінарну послідовність довжини M біт.

2.3. Вбудувати повідомлення методом k -LSB в кожний з контейнерів, де $k \in \{1, 2, 3, 4, 5, 6\}$, обираючи стеганошлях випадковим чином.

2.4. Для кожного стеганоповідомлення провести атаку проти вбудованого повідомлення, конкретний вид якої студент обирає сам. Це може бути:

- накладання гаусівського шуму з двома різними значеннями параметру;
- накладання мультиплікативного шуму з двома різними значеннями параметру;
- фільтрація з різними параметрами;
- розмиття (по Гауссу) з двома різними радіусами;
- стиск з двома різними показниками коефіцієнта якості

тощо.

2.5. Декодувати бінарну послідовність – додаткову інформацію з кожного спотвореного в результаті атаки стеганоповідомлення. Розрахувати показник NC за формулою (1.1). Побудувати графіки залежності значення NC від k для кожного значення параметру атаки для кожного контейнера. Проаналізувати отримані результати, пояснити їх. Чи відповідають отримані результати теоретичним очікуванням?

2.6. Визначити найкраще, на Ваш погляд, значення k для організації прихованого каналу зв'язку в застосованих умовах. Чи однаковим буде це значення для ЦЗ з папок «А», «Б»? Пояснити.

Контрольні запитання:

1. Чому рекомендовані значення k будуть розрізнятися для контейнерів з папок «А», «Б»?
2. Надайте пропозиції щодо підвищення стійкості методу модифікації найменшого значущого біта до атак проти вбудованого повідомлення.
3. Чому, не дивлячись на нестійкість методу модифікації найменшого значущого біта до атак проти вбудованого повідомлення він залишається широко застосовуваним?

Варіант 4: Дослідження впливу використовуваної для вбудови додаткової інформації колірної компоненти кольорового зображення на стійкість отриманого стеганоповідомлення до атак проти вбудованого повідомлення.

1. Задача дослідження

Дослідити залежність стійкості LSB-методу до атак проти вбудованого повідомлення від використовуваної для вбудови додаткової інформації колірної компоненти кольорового ЦЗ-контейнера.

2. Завдання

2.1. Обрати кольорові ЦЗ-контейнери: студент А з папки «А»; студент Б з папки «Б».

2.2. Сформувати секретне повідомлення – бінарну послідовність довжини M біт.

2.3. Розкласти RGB-зображення на три окремі матриці – колірні компоненти: R, G, B.

2.4. Вбудувати сформовану на кроці 2.2 бінарну послідовність методом модифікації найменшого значущого біта почергово:

- Тільки в канал «Red»;
- Тільки в канал «Green»;
- Тільки в канал «Blue».

В кожному разі зібрати зображення-стеганоповідомлення відповідно зі схемою RGB.

2.5. Піддати стеганоповідомлення атаці проти вбудованого повідомлення, конкретний вид якої студент обирає сам. Це може бути:

- накладання гаусівського шуму з двома різними значеннями параметру;
- накладання мультиплікативного шуму з двома різними значеннями параметру;
- фільтрація з різними параметрами;
- розмиття (по Гауссу) з двома різними радіусами;
- стиск з двома різними показниками коефіцієнта якості

тощо.

2.6. Декодувати бінарну послідовність – додаткову інформацію з кожного спотвореного в результаті атаки стеганоповідомлення, враховуючи в яку колірну компоненту відбувалася вбудова. Розрахувати показник NC за формулою (1.1).

2.7. Виконати перетворення поданих контейнерів зі схеми збереження RGB у схему YCbCr, використовуючи:

$$Y = 0.299R + 0.587G + 0.114B;$$

$$Cb = 128 - 0.168R - 0.331G + 0.5B;$$

$$Cr = 128 + 0.5R - 0.418G - 0.081B.$$

Вбудувати сформовану на кроці 2.2 бінарну послідовність методом модифікації найменшого значущого біта в канал Y (яскравість).

2.8. Виконати зворотне перетворення отриманої стеганоповідомлення в схему RGB для візуалізації результату стеганоперетворення:

$$R = Y + 1.402 (Cr - 128);$$

$$G = Y - 0.344136 (Cb - 128) - 0.714136 (Cr - 128);$$

$$B = Y + 1.772 (Cb - 128).$$

2.9. Піддати стеганоповідомлення той самі атаці проти вбудованого повідомлення, що вже застосовувалася на кроці 2.5.

2.10. Декодувати бінарну послідовність – додаткову інформацію з кожного спотвореного в результаті атаки стеганоповідомлення. Розрахувати показник NC за формулою (1.1).

Занести ваші результати у відповідну таблицю.

Значення NC для ЦЗ-контейнерів з папки «А»				Значення NC для ЦЗ-контейнерів з папки «Б»			
RGB			YCbCr	RGB			YCbCr
R	G	B		R	G	B	

Проаналізувати отримані результати.

2.9. Виокремити, якщо це можливо, таку колірну складову кольорового зображення, яка є найбільш придатною для вбудови додаткової інформації з точки зору забезпечення стійкості отриманого стеганоповідомлення до атак. Поясніть свій висновок. Чи залежить Ваш висновок від того, які ЦЗ ви обирали як контейнери (папки «А», «Б»)

2.10. Дослідити, як відіб'ється перехід цифрового кольорового зображення з схеми збереження RGB у YCbCr на властивостях отриманого стеганоповідомлення (в сенсі стійкості).

2.11. На основі проведеного дослідження надати рекомендації по використанню кольорових ЦЗ в якості контейнерів в різних схемах збереження (RGB, YCbCr).

Контрольні запитання:

1. Яким буде канал Y в схемі YCbCr з точки зору стійкості до атак проти вбудованого повідомлення в порівнянні з каналами R, G, B в схемі RGB? Відповідь пояснити.
2. Як в якості контейнера саме Ви будете використовувати кольорове ЦЗ? Відповідь пояснити.

ПРАКТИЧНЕ ЗАВДАННЯ №2

Тема: ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ МЕТОДУ КОХА І ЖАО, ЩО ВИКОНУЄ СТЕГАНОПЕРЕТВОРЕННЯ У ЧАСТОТНІЙ ОБЛАСТІ ЦИФРОВОГО КОНТЕНТУ

Мета: Дослідити вплив параметрів методу Коха і Жао на статистичні, візуальні характеристики матриці цифрового зображення-стеганоповідомлення, а також характеристики його чутливості до збурних дій.

Практичне завдання №2 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Теоретичні відомості

Метод відносної заміни величин коефіцієнтів дискретного косинусного перетворення (метод Коха й Жао) - це один з найпоширеніших на сьогодні методів приховання конфіденційної інформації в частотній області зображення, який полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП), є одним зі стеганографічних методів, які позиціонуються, як стійкі до незначних атак проти вбудованого повідомлення, зокрема стиску.

На початковому етапі первинне зображення стандартним чином розбивається на $l \times l$ –блоки. До кожного блоку, який будемо позначати В, застосовується ДКП, тим самим здійснюючи переведення кожного блоку із просторової в частотну область. У результаті виходить $l \times l$ –блок коефіцієнтів ДКП. Кожний блок призначено для приховання одного біта ДІ.

Розглянемо докладно реалізацію методу, в якій для вбудови біта ДІ використовуються 2 коефіцієнта ДКП.

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 (u_1, v_1) і (u_2, v_2) в масивах коефіцієнтів ДКП:

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

На практиці, як правило, обираються такі індекси, що відповідають середньочастотним коефіцієнтам ДКП.

Нехай у процесі стеганоперетворення треба вбудувати черговий біт $b_k \in \{0,1\}$ ДІ. Відповідно до секретного ключа для цього вибирається блок B ЦЗ-контейнера. Відповідний йому блок коефіцієнтів ДКП позначимо $B^{ДКП}$:

$$B^{ДКП} = \begin{bmatrix} b_{11}^{ДКП} & b_{12}^{ДКП} & \dots & b_{1l}^{ДКП} \\ b_{21}^{ДКП} & b_{22}^{ДКП} & \dots & b_{2l}^{ДКП} \\ \dots & \dots & \dots & \dots \\ b_{l1}^{ДКП} & b_{l2}^{ДКП} & \dots & b_{ll}^{ДКП} \end{bmatrix}.$$

Для вбудови b_k використовуються коефіцієнти $b_{u_1, v_1}^{ДКП}$, $b_{u_2, v_2}^{ДКП}$. Вбудова біта b_k відбувається таким чином: якщо $b_k = 0$, то різниця абсолютних значень використовуваних для вбудовування коефіцієнтів ДКП роблять більше деякої заданої додатної величини P , а якщо $b_k = 1$, то ця різниця робиться менше $-P$:

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

Таким чином, первинне зображення спотворюється за рахунок внесення змін у коефіцієнти ДКП, якщо їх відносні величини не відповідають приховуваному біту.

Після відповідного внесення корекції в значення коефіцієнтів ДКП, проводиться зворотне ДКП блоку.

У результаті пересилання стеганоповідомлення може зазнати 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:

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

де $\bar{b}_{u_1, v_1}^{ДКП}$, $\bar{b}_{u_2, v_2}^{ДКП}$ - коефіцієнти ДКП блоку можливо зміненого при передачі стеганоповідомлення.

Кількісною оцінкою ефективності декодування виступає коефіцієнт кореляції NC між вбудованою додатковою інформацією $p_1, p_2, \dots, p_t, p_i \in \{0,1\}$, $i = \overline{1, t}$, що є результатом попереднього кодування секретного повідомлення, і декодованою $\overline{p}_1, \overline{p}_2, \dots, \overline{p}_t, \overline{p}_i \in \{0,1\}$, $i = \overline{1, t}$:

$$NC = \sum_{i=1}^t p_i' \times \overline{p}_i' / t, \quad (2.1)$$

де $p_i' = 1, \overline{p}_i' = 1$, якщо $p_i = 1, \overline{p}_i = 1$, і $p_i' = -1, \overline{p}_i' = -1$, якщо $p_i = 0, \overline{p}_i = 0$. Чим менше NC , тим більшим є ступінь чутливості стеганоповідомлення.

Властивості стеганоповідомлення очевидно залежать від використовуваних параметрів методу Коха і Жао:

- розміру блоків l ;
- індексів (u_1, v_1) і (u_2, v_2) коефіцієнтів ДКП блоку, що задіюються для вбудови біта ДІ;
- значення P .

Варіанти практичного завдання № 2

Кожен варіант розрахований на команду з двох студентів: студент А, студент Б.

Варіант 1: Дослідження властивостей методу Коха і Жао залежно від розміру блоків контейнера.

1. Задача дослідження

Дослідити залежність візуальної якості формованого стеганоповідомлення від розміру l квадратних непересічних блоків, на які ЦЗ розбивається стандартним чином, для встановлення найбільш придатного значення l для організації стеганоперетворення. Встановити, чи можна визначити цей параметр так, щоб він забезпечував візуальну якість незалежно від властивостей контейнера.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Кожне ЦЗ розбивається стандартним чином на непересічні $l \times l$ – блоки, при цьому $l \in \{4, 8, 16\}$.

2.3. Сформувати секретні повідомлення – бінарні послідовності таким чином, щоб кількість їх біт дорівнювала кількості $l \times l$ – блоків контейнера, $l \in \{4, 8, 16\}$.

2.4. Вбудувати отримані повідомлення методом Коха і Жао в кожний з контейнерів при розбивці $l \times l$ – блоки, $l \in \{4, 8, 16\}$ (в кожний блок вбудовується 1 біт ДІ). При цьому використовувати **строго** середньочастотні коефіцієнти ДКП, $P=25$.

Таким чином для кожного контейнера отримується 3 стеганоповідомлення.

2.5. Для кожного стеганоповідомлення розрахувати показник візуального спотворення PSNR (Peak Signal-to-Noise Ratio). Побудувати графіки залежності значення PSNR від l (для ЦЗ з папки «А» і окремо з папки «Б»).

2.6. Оцінити візуальну якість всіх отриманих стеганоповідомлень шляхом суб'єктивного ранжування (враховуючи думку всіх зацікавлених сторін). Порівняти суб'єктивну і кількісну оцінку візуальної якості. Занести ваші результати у відповідну таблицю.

Оцінка візуальної якості ЦЗ з папки «А»		Оцінка візуальної якості ЦЗ з папки «Б»	
PSNR	Шляхом суб'єктивного ранжування	PSNR	Шляхом суб'єктивного ранжування

Пояснити отримані результати.

2.7. Визначити (якщо можливо) таке значення l , при якому виникають артефакти на ЦЗ-стеганоповідомленні. Чи однаковим буде це значення для ЦЗ з папок «А», «Б»? Пояснити отримані результати.

2.8. Побудувати гістограми значень яскравості поданих контейнерів і відповідних їм стеганоповідомлень. Прокоментувати властивості отриманих гістограм.

2.9. Сформулювати висновки, рекомендації по використанню контейнерів, методу Коха і Жал для різних розмірів блоків по результатах проведеного дослідження.

Контрольні запитання:

1. Чи відповідає отримане значення PSNR візуальному суб'єктивному сприйняттю стеганоповідомлення? Поясніть свою відповідь.
2. Сформулюйте пропозиції щодо покращення методу Коха і Жао в сенсі збереження надійності сприйняття формованого повідомлення.
3. В яких умовах працювання стеганосистеми Ви будете застосовувати метод Коха і Жао? Пояснити відповідь.

Варіант 2: Дослідження властивостей методу Коха і Жао залежно від обраних для вбудови ДІ коефіцієнтів ДКП блоків (візуальної якості стеганоповідомлення).

1. Задача дослідження

Дослідити залежність візуальної якості формованого стеганоповідомлення від обраних для вбудови ДІ коефіцієнтів ДКП блоків, для встановлення найбільш придатних для організації стеганоперетворення. Встановити, чи можна визначити цей параметр так, щоб він забезпечував візуальну якість незалежно від властивостей контейнера.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Кожне ЦЗ розбивається стандартним чином на непересічні 8×8 – блоки.

2.3. Сформувати секретні повідомлення – бінарні послідовності таким чином, щоб кількість їх біт дорівнювала кількості 8×8 – блоків контейнера.

2.4. Вбудувати ДІ методом Коха і Жао в кожний з контейнерів, використовуючи три різних варіанта пар (u_1, v_1) і (u_2, v_2) коефіцієнтів ДКП блоку, що задіюються для вбудови біта ДІ. Таким чином для кожного контейнера отримується 3 стеганоповідомлення.

2.5. Для кожного стеганоповідомлення розрахувати показник візуального спотворення PSNR (Peak Signal-to-Noise Ratio).

2.6. Оцінити візуальну якість всіх отриманих стеганоповідомлень шляхом суб'єктивного ранжування (враховуючи думку всіх зацікавлених сторін). Порівняти суб'єктивну і кількісну оцінку візуальної якості. Занести ваші результати у відповідну таблицю.

Оцінка візуальної якості ЦЗ з папки «А»			Оцінка візуальної якості ЦЗ з папки «Б»		
Коефіцієнти ДКП	PSNR	Шляхом суб'єктивного ранжування	Коефіцієнти ДКП	PSNR	Шляхом суб'єктивного ранжування

Пояснити отримані результати.

2.7. Визначити (якщо можливо) такі значення індексів (u_1, v_1) і (u_2, v_2) , при яких виникають артефакти на ЦЗ-стеганоповідомленні. Чи однаковими будуть визначені індекси для ЦЗ з папок «А», «Б»? Пояснити отримані результати.

2.8. Побудувати гістограми значень яскравості поданих контейнерів і відповідних їм стеганоповідомлень. Прокоментувати властивості отриманих гістограм.

2.9. Сформулювати висновки, рекомендації по використанню контейнерів, методу Коха і Жао для різних значень індексів (u_1, v_1) і (u_2, v_2) по результатах проведеного дослідження.

Контрольні запитання:

1. Чи відповідає отримане значення PSNR візуальному суб'єктивному сприйняттю стеганоповідомлення? Поясніть свою відповідь.
2. Сформулюйте пропозиції щодо покращення методу Коха і Жао в сенсі збереження надійності сприйняття формованого повідомлення.
3. В яких умовах працювання стеганосистеми Ви будете застосовувати метод Коха і Жао, корегуючи індекси (u_1, v_1) і (u_2, v_2) ? Пояснити відповідь.

Варіант 3: Дослідження властивостей методу Коха і Жао залежно від параметру P , що використовується для коригування коефіцієнтів ДКП при вбудові ДІ.

1. Задача дослідження

Дослідити залежність візуальної якості формованого стеганоповідомлення від значення P , для встановлення найбільш придатного значення для організації стеганоперетворення. Встановити, чи можна визначити цей параметр так, щоб він забезпечував візуальну якість незалежно від властивостей контейнера.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Кожне ЦЗ розбивається стандартним чином на непересічні 8×8 – блоки.

2.3. Сформувати секретні повідомлення – бінарні послідовності таким чином, щоб кількість їх біт дорівнювала кількості 8×8 – блоків контейнера.

2.4. Вбудувати отримані повідомлення методом Коха і Жао в кожний з контейнерів при розбивці 8×8 – блоки (в кожний блок вбудовується 1 біт ДІ), використовуючи **строго** середньочастотні коефіцієнти ДКП. При цьому обирати різні значення $P \in \{25, 45, 65\}$. Таким чином для кожного контейнера отримується 3 стеганоповідомлення.

2.5. Для кожного стеганоповідомлення розрахувати показник візуального спотворення PSNR (Peak Signal-to-Noise Ratio). Побудувати графіки залежності значення PSNR від P (для ЦЗ з папки «А» і окремо з папки «Б»).

2.6. Оцінити візуальну якість всіх отриманих стеганоповідомлень шляхом суб'єктивного ранжування (враховуючи думку всіх зацікавлених сторін). Порівняти суб'єктивну і кількісну оцінку візуальної якості. Занести ваші результати у відповідну таблицю.

Оцінка візуальної якості ЦЗ з папки «А»		Оцінка візуальної якості ЦЗ з папки «Б»	
PSNR	Шляхом суб'єктивного ранжування	PSNR	Шляхом суб'єктивного ранжування

Пояснити отримані результати.

2.7. Визначити (якщо можливо) таке значення P , при якому виникають артефакти на ЦЗ-стеганоповідомленні. Чи однаковим буде це значення для ЦЗ з папок «А», «Б»? Пояснити отримані результати.

2.8. Побудувати гістограми значень яскравості поданих контейнерів і відповідних їм стеганоповідомлень. Прокоментувати властивості отриманих гістограм.

2.9. Сформулювати висновки, рекомендації по використанню контейнерів, методу Коха і Жао для різних значень параметру P по результатах проведеного дослідження.

Контрольні запитання:

1. Чи відповідає отримане значення PSNR візуальному суб'єктивному сприйняттю стеганоповідомлення? Поясніть свою відповідь.
2. Сформууйте пропозиції щодо покращення методу Коха і Жао в сенсі збереження надійності сприйняття формованого повідомлення.
3. В яких умовах працювання стеганосистеми Ви будете застосовувати метод Коха і Жао? Пояснити відповідь.

Варіант 4: Дослідження властивостей методу Коха і Жао залежно від обраних для вбудови ДІ коефіцієнтів ДКП блоків (стійкості до атаки стиском).

1. Задача дослідження

Дослідити залежність стійкості до атаки стиском методу Коха і Жао від обраних для вбудови ДІ коефіцієнтів ДКП блоків, для встановлення найбільш придатних для організації стеганоперетворення. Встановити, чи можна визначити цей параметр так, щоб він забезпечував стійкість до атаки стиском незалежно від властивостей контейнера.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Кожне ЦЗ розбивається стандартним чином на непересічні 8×8 – блоки.

2.3. Сформувати секретні повідомлення – бінарні послідовності таким чином, щоб кількість їх біт дорівнювала кількості 8×8 – блоків контейнера.

2.4. Вбудувати ДІ методом Коха і Жао в кожний з контейнерів, використовуючи три різних варіанта пар (u_1, v_1) і (u_2, v_2) коефіцієнтів ДКП блоку, що задіюються для вбудови біта ДІ ($P=25$). Таким чином для кожного контейнера отримується 3 стеганоповідомлення.

2.5. Кожне стеганоповідомлення піддати атаці стиском (збереження в формат Jpeg з коефіцієнтом якості $QF \in \{85, 75, 65\}$).

2.6. Здійснити декодування ДІ зі спотворених контейнерів, розраховуючи кількісний показник ефективності декодування NC за формулою (2.1). Для кожного стеганоповідомлення побудувати графік залежності NC від QF.

Отримані результати звести в таблицю:

Оцінка стійкості стеганоповідомлення (ЦЗ з папки «А»)			Оцінка стійкості стеганоповідомлення (ЦЗ з папки «Б»)		
Коефіцієнти ДКП	NC	QF	Коефіцієнти ДКП	NC	QF

Пояснити отримані результати.

2.7. Визначити такі значення індексів (u_1, v_1) і (u_2, v_2) , при яких стійкість стеганоповідомлення до стиску є максимальна. Чи однаковими будуть визначені індекси для ЦЗ з папок «А», «Б»? Пояснити отримані результати.

2.8. Побудувати гістограми значень яскравості поданих контейнерів і відповідних їм стеганоповідомлень. Прокоментувати властивості отриманих гістограм.

2.9. Сформулювати висновки, рекомендації по використанню контейнерів, методу Коха і Жао для різних значень індексів (u_1, v_1) і (u_2, v_2) по результатах проведеного дослідження.

Контрольні запитання:

1. Чи відповідають отримані в результаті дослідження кількісні результати Вашим теоретичним очікуванням стосовно стійкості метода Коха і Жао до атаки стиском? Поясніть свою відповідь.
2. Сформулюйте пропозиції щодо покращення методу Коха і Жао в сенсі підвищення стійкості стеганоповідомлення до атаки стиском.
3. В яких умовах працювання стеганосистеми Ви будете застосовувати метод Коха і Жао, корегуючи індекси (u_1, v_1) і (u_2, v_2) ? Пояснити відповідь.

ПРАКТИЧНЕ ЗАВДАННЯ №3

Тема: СТЕГАНОАНАЛІЗ МЕТОДУ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА, ЩО ВИКОНУЄ СТЕГАНОПЕРЕТВОРЕННЯ У ПРОСТОРОВІЙ ОБЛАСТІ ЦИФРОВОГО КОНТЕНТУ

Мета: Набуття практичних навичок застосування методів стеганоаналізу просторової області, що дозволить магістранту виявляти сліди прихованого впровадження інформації за методом найменшого значущого біта (LSB) та оцінювати ефективність детекторів за допомогою числових критеріїв.

Практичне завдання №3 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Варіанти практичного завдання №3

Кожен варіант розрахований на команду з двох-чотирьох студентів: студент А, студент Б.

Варіант 1: Дослідження k -LSB-методу в просторовій області в сенсі забезпечення стійкості до виявлення.

1. Задача дослідження

При фіксованому секретному повідомленні (бінарній послідовності, що є результатом роботи прекодера стеганосистеми) довжиною M біт є два шляхи:

3. Використання 1-LSB-методу, тобто задіяти M пікселів ЦЗ-контейнера, змінивши в кожному лише 1 найменший значущий біт.
4. Використання k -LSB-методу, тобто задіяти M/k пікселів, змінивши в кожному k молодших бітів.

Дослідити: залежність стійкості до виявлення від k для ЦЗ-контейнерів, що мають різні властивості.

Визначити поріг пропускнуєї спроможності, при якому LSB-вбудовування стає статистично помітним.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Сформулювати секретне повідомлення – бінарну послідовність довжини M біт.

2.3. Вбудувати повідомлення методом k -LSB в кожний з контейнерів, де $k \in \{1, 2, 3, 4, 5, 6\}$, обираючи стеганошлях випадковим чином.

2.4. Виділити та візуалізувати бітові площини 0,1,2,3,4,5 для оригінального контейнера та стеганоповідомлення. Дослідити їх особливості. Визначити, для якого значення $k \in \{1, 2, 3, 4, 5, 6\}$ метод k -LSB є найбільш стійким/нестійким до стеганоаналізу методом візуального аналізу бітових зрізів. Пояснити отримані результати.

2.5. Дослідити зв'язок між значеннями PSNR (*Завдання 1*) і стійкістю до виявлення прихованого каналу.

2.6. Побудувати гістограми яскравості для декількох вузьких діапазонів значень (наприклад, [120, 130]). Проаналізувати появу «парних значень» при зростанні k .

2.7. Збільшити поступово пропускну спроможність прихованого каналу, збільшуючи довжину бінарної послідовності – додаткової інформації: $1.2 \cdot M$ біт, $1.5 \cdot M$ біт, $1.8 \cdot M$ біт. Дослідити, при якій пропускній спроможності (біт/піксель) метод стає «прозорим» для виявлення.

2.8. Сформулювати висновки, рекомендації по використанню контейнерів, умов використання k -LSB-методу по результатах проведеного дослідження.

Контрольні запитання:

4. Чи можна вважати метод візуального аналізу бітових зрізів ефективним стеганоаналітичним методом при сучасному стані стеганографії? Пояснити відповідь.
5. Чи має сенс застосовувати нестійкі до виявлення стеганоаналітичні методи з малою пропускну спроможністю прихованого каналу зв'язку? Відповідь пояснити.
6. Який з k -LSB-методів будете використовувати за необхідності Ви з урахуванням наявності пасивного порушника? Поясніть свою відповідь.

Варіант 2: Дослідження впливу використовуваної для вбудови додаткової інформації колірної компоненти кольорового зображення на стійкість до виявлення.

1. Задача дослідження

Дослідити, чи можна виокремити таку колірну складову кольорового зображення, яка є найбільш придатною для вбудови додаткової інформації з точки зору забезпечення стійкості до виявлення прихованого каналу; як відіб'ється перехід цифрового кольорового зображення з схеми збереження RGB у YCbCr на властивостях отриманого стеганоповідомлення у сенсі стійкості до виявлення прихованого каналу.

2. Завдання

2.1. Обрати кольорові ЦЗ-контейнери: студент А з папки «А»; студент Б з папки «Б».

2.2. Сформувати секретне повідомлення – бінарну послідовність довжини M біт.

2.3. Розкласти RGB-зображення на три окремі матриці – колірні компоненти: R, G, B.

2.4. Вбудувати сформовану на кроці 2.2 бінарну послідовність методом модифікації найменшого значущого біта почергово:

- Тільки в канал «Red»;
- Тільки в канал «Green»;
- Тільки в канал «Blue».

2.5. Для кожного каналу виділити та візуалізувати бітові площини 0,1,2,3,4,5 для оригінального контейнера та стеганоповідомлення. Дослідити їх особливості. Визначити, для якого колірного каналу LSB-метод є найбільш стійким/нестійким до стеганоаналізу методом візуального аналізу бітових зрізів. Пояснити отримані результати.

2.6. Дослідити зв'язок між значеннями PSNR (*Завдання 1*) і стійкістю до виявлення прихованого каналу.

2.7. Побудувати гістограми яскравості для декількох вузьких діапазонів значень (наприклад, [120, 130]) для кожного колірного каналу. Проаналізувати появу «парних значень» при зростанні k.

2.8. Збільшити поступово пропускну спроможність прихованого каналу, збільшуючи довжину бінарної послідовності – додаткової інформації: $1.2 \cdot M$ біт, $1.5 \cdot M$ біт, $1.8 \cdot M$ біт. Дослідити для кожного колірного каналу, при якій пропускну спроможності (біт/піксель) метод стає «прозорим» для виявлення.

2.9. Виконати перетворення поданих контейнерів зі схеми збереження RGB у схему YCbCr, використовуючи:

$$\begin{aligned}Y &= 0.299R + 0.587G + 0.114B; \\C_b &= 128 - 0.168R - 0.331G + 0.5B; \\C_r &= 128 + 0.5R - 0.418G - 0.081B.\end{aligned}$$

Вбудувати сформовану на кроці 2.2 бінарну послідовність методом модифікації найменшого значущого біта в канал Y (яскравість).

2.10. Для каналу Y проробити кроки 2.5-2.8.

2.11. Виокремити таку колірну складову кольорового зображення, яка є найбільш придатною для вбудови додаткової інформації з точки зору забезпечення стійкості до виявлення. Поясніть свій висновок. Чи залежить Ваш висновок від того, які ЦЗ ви обирали як контейнери (папки «А», «Б»)

2.12. Сформулювати висновки, рекомендації по використанню контейнерів - кольорових ЦЗ в різних схемах збереження (RGB, YCbCr), умов використання LSB-методу по результатах проведеного дослідження

Контрольні запитання:

4. Чи можна вважати метод візуального аналізу бітових зрізів ефективним стеганоаналітичним методом при сучасному стані стеганографії? Пояснити відповідь.
5. Чи має сенс застосовувати нестійкі до виявлення стеганоаналітичні методи з малою пропускну спроможністю прихованого каналу зв'язку? Відповідь пояснити.

6. Який з k -LSB-методів будете використовувати за необхідності Ви з урахуванням наявності пасивного порушника? Поясніть свою відповідь.

ПРАКТИЧНЕ ЗАВДАННЯ №4

Тема: ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИЯВЛЕННЯ НАЯВНОСТІ ДОДАТКОВОЇ ІНФОРМАЦІЇ В ЦИФРОВОМУ ЗОБРАЖЕННІ, ВБУДОВАНОЇ МЕТОДОМ КОХА І ЖАО

Мета: Набуття практичних навичок виявлення наявності прихованої інформації, вбудованої в частотну область контейнера за методом Коха і Жао, що дозволяє магістранту досліджувати специфічні структурні аномалії та ознаки присутності додаткової інформації на основі аналізу взаємозв'язку коефіцієнтів дискретного косинусного перетворення.

Практичне завдання №4 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Варіанти практичного завдання № 4

Кожен варіант розрахований на команду з двох-чотирьох студентів: студент А, студент Б.

Варіант 1: Дослідження стійкості методу Коха і Жао до виявлення залежно від розміру блоків контейнера.

1. Задача дослідження

Дослідити вплив параметрів вбудовування додаткової інформації на статистику коефіцієнтів ДКП.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Кожне ЦЗ розбивається стандартним чином на непересічні $l \times l$ – блоки, при цьому $l \in \{4, 8, 16\}$.

2.3. Сформувані секретні повідомлення – бінарні послідовності таким чином, щоб кількість їх біт дорівнювала кількості $l \times l$ – блоків контейнера, $l \in \{4, 8, 16\}$.

2.4. Вбудувати отримані повідомлення методом Коха і Жао в кожний з контейнерів при розбивці $l \times l$ – блоки, $l \in \{4, 8, 16\}$ (в кожний блок вбудовується 1 біт ДІ). При цьому використовувати **строго** середньочастотні коефіцієнти

ДКП, $P=25$. Таким чином для кожного контейнера отримується 3 стеганоповідомлення.

2.5. Побудувати та дослідити гістограми вибраних для вбудови ДІ середньочастотних коефіцієнтів (i, j) блоків до та після вбудовування.

2.6. Визначити, чи залежить успішність виявлення наявності ДІ від розміру блоку.

2.8. Виділити та візуалізувати бітові площини 0,1,2,3,4,5 для оригінального контейнера та стеганоповідомлення. Дослідити їх особливості (при наявності).

2.9. Сформулювати висновки та рекомендації щодо вибору параметрів («розмір блоку», (i, j)), які зменшують ризик виявлення прихованого каналу.

Контрольні запитання:

4. Яку роль відіграє параметр «розмір блоку» у методі Коха і Жао з точки зору балансу між «стійкістю до стиску» та «непомітністю для стеганоаналізу»?
5. Поясніть концепцію «стеганографічної вартості»: чому не всі коефіцієнти ДКП однаково придатні для вбудовування ДІ?
6. Чи має сенс використовувати метод бітових площин у випадку, коли стеганоперетворення відбувається в частотній області? Відповідь пояснити.

Варіант 2: Дослідження стійкості методу Коха і Жао до виявлення залежно від параметру P , що використовується для коригування коефіцієнтів ДКП при вбудові ДІ.

1. Задача дослідження

Дослідити вплив параметрів вбудовування додаткової інформації на статистику коефіцієнтів ДКП.

2. Завдання

2.1. Обрати ЦЗ-контейнери: студент А з папки «А», студент Б з папки «Б», переводячи їх в зображення в градаціях сірого.

2.2. Кожне ЦЗ розбивається стандартним чином на непересічні 8×8 – блоки.

2.3. Сформувати секретні повідомлення – бінарні послідовності таким чином, щоб кількість їх біт дорівнювала кількості 8×8 – блоків контейнера.

2.4. Вбудувати отримані повідомлення методом Коха і Жао в кожний з контейнерів при розбивці 8×8 – блоки (в кожний блок вбудовується 1 біт ДІ), використовуючи **строго** середньочастотні коефіцієнти ДКП. При цьому обирати різні значення $P \in \{25, 45, 65\}$. Таким чином для кожного контейнера отримується 3 стеганоповідомлення.

2.5. Побудувати та дослідити гістограми вибраних для вбудови ДІ середньочастотних коефіцієнтів (i, j) блоків до та після вбудовування.

2.6. Визначити, чи залежить успішність виявлення наявності ДІ від значення P .

2.8. Виділити та візуалізувати бітові площини 0,1,2,3,4,5 для оригінального контейнера та стеганоповідомлення. Дослідити їх особливості (при наявності).

2.9. Сформулювати висновки та рекомендації щодо вибору параметрів (P (i, j)), які зменшують ризик виявлення прихованого каналу.

Контрольні запитання:

1. Яку роль відіграє параметр P у методі Коха і Жао з точки зору балансу між «стійкістю до стиску» та «непомітністю для стеганоаналізу»?
2. Поясніть концепцію «стеганографічної вартості»: чому не всі коефіцієнти ДКП однаково придатні для вбудовування ДІ?
3. Чи має сенс використовувати метод бітових площин у випадку, коли стеганоперетворення відбувається в частотній області? Відповідь пояснити.

Література

Базова

1. Г.Ф. Конахович, Д.О. Прогонов, О.Ю. Пузиренко, *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник*. Київ: Alex Print Centre, 2018. <https://books.google.com.ua/books?id=-clcDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false>
2. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с
3. Браїловський М.М. Аналіз кіберзахищеності інформаційних систем: монографія/ Браїловський М.М., Кобозєва А.А., Хорошко В.О., Хохлачева Ю.Є. – К.: ФОП Ямчинський О.В., 2021. – 360 с.

Допоміжна

1. Bobok I.I., Kobozieva A.A. Localization of Disturbance Region of Formal Parameters of Steganographic Cover to Ensure Steganosystem Stability. *Radioelectronics and Communications Systems*. 2024, 67(8), pp. 396-409.
2. Kobozieva A.A. et al. Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel/ PROBLEMELE ENERGETICII REGIONALE. 2(66). 2025 P.90-104 <https://journal.ie.asm.md/ru/contents/electronni-jurnal-266-2025>
3. Kobozieva A.A. et al. Increasing the Resistance of the Steganosystem to Attacks Against an Embedded Message by Selection of Container Blocks / 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT), Lviv, Ukraine, 2024, pp. 264-269, doi: 10.1109/ATIT64324.2024.11222497
4. Kobozieva A.A. et al. Steganographic method with code control of information embedding based on multi-level code words/Radioelectronics and Communications Systems. 2023 <https://radioelektronika.org/article/view/S0735272723040052>