Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

ПРИХОВУВАННЯ ДАНИХ У ЧАСТОТНІЙ ОБЛАСТІ НЕРУХОМИХ ЗОБРАЖЕНЬ НА ОСНОВІ КОДУВАННЯ РІЗНИЦІ АБСОЛЮТНИХ ЗНАЧЕНЬ КОЕФІЦІЄНТІВ ДИСКРЕТНО-КОСИНУСНОГО ПЕРЕТВОРЕННЯ

Методичні рекомендації
до лабораторної роботи з дисципліни «Стеганографія»
для студентів спеціальності 125 «Кібербезпека»

Харків – 2019

УДК 004.415.24 (075.8)
П 77

Рецензенти:

В. А. Краснобаєв – доктор технічних наук, професор, професор кафедри електроніки і управляючих систем Харківського національного університету імені В. Н. Каразіна;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки Харківського національного університету імені В. Н. Каразіна.

Затверджено до друку рішенням Науково-методичної ради Харківського національного університету імені В. Н. Каразіна (протокол № 1 від 30.10.2019 р.)

П 77 **Приховування** даних у частотній області нерухомих зображень на основі кодування різниці абсолютних значень коефіцієнтів дискретно-косинусного перетворення : методичні рекомендації до лабораторної роботи з дисципліни «Стеганографія» для студентів спеціальності 125 «Кібербезпека» / уклад. О. О. Кузнецов, М. О. Полуяненко, Т. Ю. Кузнецова. – Харків : ХНУ імені В. Н. Каразіна, 2019. – 52 с.

Методичні рекомендації розроблено для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека». Матеріали методичних рекомендацій мають допомогти студентам усвідомити специфіку безпеки інформаційних і комунікаційних систем та особливості професійної наукової діяльності у галузі захисту інформації. Передбачається, що в результаті навчання студенти оволодіють початковими навичками роботи з дисципліни «Стеганографія», вироблять ставлення до використання методів та принципів приховування даних, набудуть практичних вмінь та навичок щодо розробки стеганографічних систем.

УДК 004.415.24 (075.8)

ЗМІСТ

1. МЕТА І ЗАВДАННЯ ЛАБОРАТОРНОЇ РОБОТИ

Мета роботи: закріпити теоретичні знання з теми «Приховування даних у частотній області нерухомих зображень», набути практичних вмінь та навичок з розробки стеганографічних систем, дослідити властивості стеганографічних методів, заснованих на низькорівневих властивостях зорової системи людини (ЗСЛ), зокрема частотної чутливості.

Лабораторна робота № 4 виконується в середовищі символьної математики MathCAD версії 12 або вище.

Завдання лабораторної роботи

1. Реалізувати у середовищі символьної математики MathCAD алгоритми прямого та зворотного дискретно-косинусного перетворення. Дослідити ефект частотної чуттєвості зорової системи людини, а саме як зміна коефіцієнтів дискретно-косинусного перетворення у різних частотних областях впливає на наявність видимих викривлень зображень.

2. Реалізувати у середовищі символьної математики MathCAD алгоритми приховування даних у частотну область нерухомих зображень шляхом кодування різниці абсолютних значень коефіцієнтів дискретно-косинусного перетворення (метод Коха–Жао). Виконати зорове порівняння порожнього та заповненого контейнера та зробити відповідні висновки. Реалізувати алгоритми вилучення даних із частотної області зображень методом Коха–Жао.

3. Реалізувати імітацію стеганоатаки на основі стискання зображення алгоритмом JPEG. Дослідити ймовірнісні властивості реалізованих алгоритмів до та після реалізації атаки, а саме отримати емпіричні залежності ймовірності правильного вилучення даних та частки внесених при цьому похибок у контейнер-зображення. Шляхом збільшення величини внесених викривлень коефіцієнтів дискретно-косинусного перетворення досягти зменшення помилки вилучення інформаційних даних навіть за імітації атаки стисканням.

4. Реалізувати у середовищі символьної математики MathCAD алгоритми приховування даних у частотну область нерухомих зображень шляхом кодування декількох різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення (удосконалений метод Кох–Жао – метод Бенгама–Мемона–Ео–Юнга). Виконати зорове порівняння порожнього та заповненого контейнера та зробити відповідні висновки. Реалізувати алгоритми вилучення даних із частотної області зображень методом Бенгама–Мемона–Ео–Юнга. Дослідити ймовірнісні властивості реалізованих алгоритмів.

5. (Додаткове завдання). Реалізувати у середовищі символьної математики MathCAD алгоритми приховування та вилучення інформаційних даних у частотну область нерухомих зображень методом Дж. Фрідріх.

2. МЕТОДИЧНІ ВКАЗІВКИ З ОРГАНІЗАЦІЇ САМОСТІЙНОЇ РОБОТИ

1. Вивчити теоретичний матеріал лекції «Приховування даних у частотній області нерухомих зображень на основі кодування різниці абсолютних значень коефіцієнтів дискретно-косинусного перетворення».

2. Вивчити матеріал основного джерела літератури (Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография): приховування даних в частотній області зображень (с. 126–179).

3. Вивчити матеріал додаткових джерел:

а) About JPEG (http://www.pcs-ip.eu/index.php/main/edu/5);

б) The Discrete Cosine Transform (http://www.cs.cf.ac.uk/Dave/Multimedia/node231.html).

4. Вивчити основні команди у середовищі символьної математики MathCAD щодо роботи із зображеннями.

5. Підготувати відповіді на контрольні запитання.

6. Підготувати бланк звіту з лабораторної роботи.

Допуск до виконання лабораторної роботи здійснюється за результатами письмового опитування.

3. ЗАГАЛЬНОТЕОРЕТИЧНІ ПОЛОЖЕННЯ ЗА ТЕМОЮ ЛАБОРАТОРНОЇ РОБОТИ

3.1. Приховування даних у частотній області зображення

Стеганографічні методи приховування даних у просторовій області зображення є нестійкими до більшості з відомих видів спотворень. Так, наприклад, використання операції компресії з втратами (щодо зображення це може бути JPEG-компресія) призводить до часткового або, що більш ймовірно, повного знищення вбудованої в контейнер інформації. Більш стійкими до різноманітних спотворень, в тому числі й компресії, є методи, які використовують для приховування даних не просторову область контейнера, а частотну.

Існує кілька способів представлення зображення в частотній області. При цьому використовується та чи інша декомпозиція зображення, що використовується в якості контейнера. Наприклад, існують методи на основі використання дискретного косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення Карунена–Лоєва і деякі інші. Подібні перетворення можуть застосовуватися або до окремих частин зображення, або до зображення в цілому.

Найбільшого поширення серед всіх ортогональних перетворень в стеганографії отримали вейвлет-перетворення і ДКП, що певною мірою

пояснюється значним поширенням їх використання під час компресії зображень. Крім того, для приховування даних доцільно застосовувати саме те перетворення зображення, якому воно буде підлягати згодом за можливої компресії. Наприклад, відомо, що алгоритм ДКП є базовим у стандарті JPEG, а вейвлет-перетворення – в стандарті JPEG2000.

Стеганоалгоритм може бути досить стійким до подальшої компресії зображення, тільки якщо він буде враховувати особливості алгоритму перспективного стиснення. При цьому, звичайно, стеганоалгоритм, в основу якого закладено вейвлет-перетворення, зовсім не обов'язково буде стійким до дискретно-косинусного алгоритму стиснення, і навпаки. Великі труднощі виникають при виборі методу стеганоперетворення під час приховування даних у потоковому відео. Причина цього – однією зі складових алгоритмів компресії відеоінформації (на додаток до компресії нерухомого кадру) є кодування векторів компенсації руху. При компресії нерухомих зображень ця компенсація відсутня за непотрібністю. Щоб бути достатньою мірою стійким, стеганоалгоритм повинен враховувати цей фактор.

Залишається також відкритим питання про існування стійкого стеганоперетворення, яке було б незалежним від застосовуваної в подальшому алгоритмі компресії.

На сьогодні відома досить велика кількість моделей, що дозволяють оцінити пропускну здатність каналу передачі прихованих даних. Розглянемо одну з них.

Нехай C – первинне зображення (контейнер-оригінал), M – повідомлення, яке підлягає приховуванню. Тоді модифіковане зображення (стеганоконтейнер) S = C + M. Також передбачається, що модифіковане зображення S візуально не відрізняється від первинного і може бути піддано в стеганоканалі компресії з втратами: $S^{\nabla} = \Theta(S)$, де $\Theta(\bullet)$ – оператор компресії.

Завдання адресата – вилучити з отриманого контейнера S^{∇} вбудовані на попередньому етапі біти даних M_i.

Постає питання – яку кількість бітів можна ефективно вбудовувати в зображення і з часом вилучити з нього за умови задовільно низької ймовірності помилок на останньому етапі. Іншими словами, яка пропускна здатність каналу передачі прихованих даних за умови наявності в каналі зв'язку певного алгоритму компресії? Блок-схема такого стеганоканала представлена на рис. 3.1.

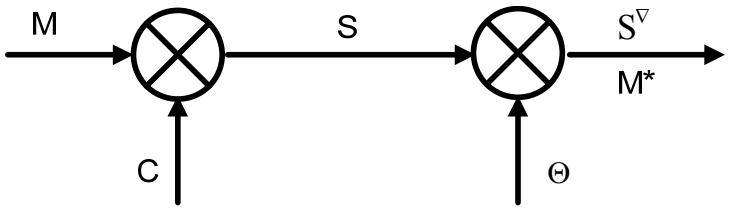


Рис. 3.1. Блок-схема стеганоканалу з атакою у вигляді компресії

Повідомлення M передається по каналу, який має два джерела «шуму»: C – зображення-контейнер і «шум» Θ, що виникає в результаті

операцій компресії/декомпресії. При цьому S^{∇} і M* – можливо спотворені стеганоконтейнер і, як результат, – оцінка корисного повідомлення.

Структурна схема стеганосистеми представлена на рис. 3.2.

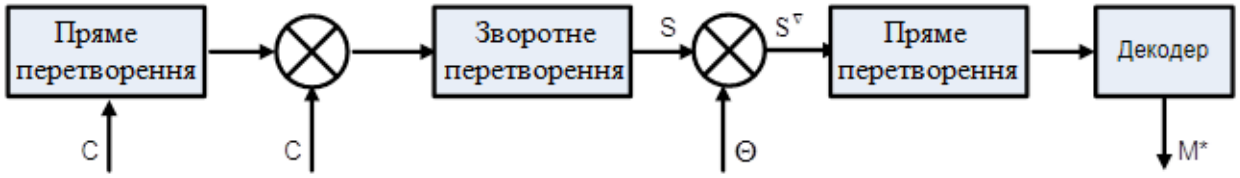


Рис. 3.2. Структурна схема стеганосистеми за наявності в стеганоканалі атаки компресії

Зображення C розкладається на D субсмуг (пряме перетворення), в кожну з яких вбудовується приховувана інформація M. Після зворотного перетворення виходить модифіковане зображення S. Після компресії/декомпресії Θ в каналі зв'язку знаходиться зображення S^{∇}, яке на приймаючій стороні знову піддається прямому перетворенню, і з кожної субсмуги D незалежно витягується приховане повідомлення – оцінка M*.

Реальні зображення не є випадковими процесами з рівномірно розподіленими значеннями величин. Відомо, і цей факт використовується в алгоритмах компресії, що велика частина енергії зображень зосереджена в низькочастотній (НЧ) області спектра. Звідси і виникає необхідність у здійсненні декомпозиції зображення на субсмуги, до яких додається стеганоповідомлення. НЧ-субсмуги містять основну частину енергії зображення і, таким чином, носять шумовий характер. Високочастотні (ВЧ) субсмуги спектра зображення найбільшим чином піддаються впливу з боку різноманітних алгоритмів обробки, таких як, наприклад, компресія або НЧ-фільтрація. Таким чином, можна зробити висновок, що для вбудовування повідомлення найоптимальнішими є середньочастотні (СЧ) субсмуги спектра зображення. Типовий розподіл шуму зображення та шуму-обробки за спектром частоти зображено на рис. 3.3.

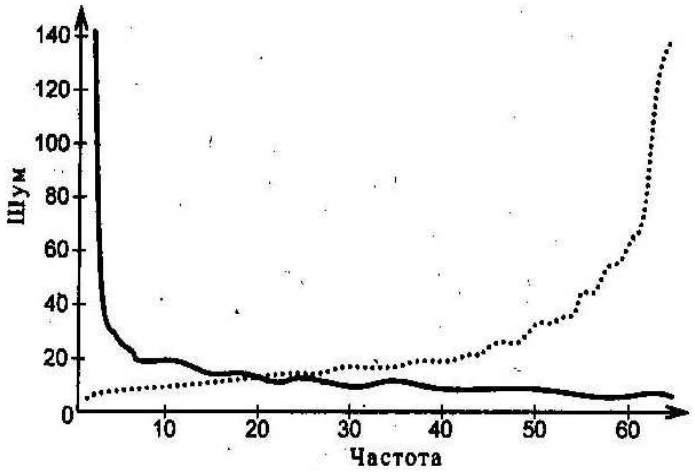


Рис. 3.3. Залежність шуму зображення (суцільна лінія) і шуму обробки (пунктирна лінія) від частоти

Стеганографічний канал можна розкласти на ряд незалежних підканалів. Таке розкладання відбувається за рахунок виконання прямого і зворотного перетворень. У кожному з D підканалів існує по два джерела шуму. Нехай, $\sigma^2_{\tilde{N},\Theta_j}$ за j = 1, ..., D – дисперсія коефі-

цієнтів перетворення (шум зображення) в кожному з підканалів. Тоді вираз для пропускної здатності каналу стеганосистеми набуде вигляду

$$B = \frac{X \cdot Y}{2 \cdot D} \cdot \sum_{j=1}^{D} \log_2 \left(1 + \frac{v_j^2}{\sigma_{C_j}^2 + \sigma_{\Theta_j}^2} \right) \text{бітів},$$

де ν_j – візуальний поріг для j-ї субсмуги;

ν_j^2 – максимально допустима енергія стеганоповідомлення, виходячи з вимог збереження візуальної якості зображення);

X і Y – піксельний розмір зображення-контейнера.

Вибір значення візуального порогу базується на урахуванні властивостей зорової системи людини. Відомо, що шум у ВЧ-областях зображення більш прийнятний, ніж в НЧ-областях.

Можна ввести деякі вагові коефіцієнти: $\nu_j^2 = \kappa \cdot \sigma_{\tilde{N},\Theta_j}^{2\cdot\alpha}$, де $0 \le \alpha \le 1$, а $\kappa << \sigma_{\tilde{N},\Theta_j} \forall$ j – константа.

Випадок, коли $\alpha = 0$, відповідає рівномірному розподілу стеганограми за всіма субсмугами. Випадок $\alpha = 1$ відповідає розподілу стеганограми відповідно до дисперсії субсмуг.

Після деяких спрощень можна отримати вираз для пропускної здатності каналу передачі прихованих даних:

$$B = \frac{X \cdot Y}{2 \cdot D} \cdot \sum_{j=1}^{D} \log_2 \left(1 + \frac{\kappa \cdot \sigma_{\tilde{N},\Theta_j}^{2\cdot\alpha}}{\sigma_{C_j}^2} \right) \approx \frac{X \cdot Y}{2 \cdot D} \log_2 \left(1 + \sum_{j=1}^{D} \frac{\kappa_1}{\sigma_{C_j}^{2\cdot(1-\alpha)}} \right). \qquad (3.1)$$

Знак наближення в виразі (3.1) є справедливим, $\kappa_1 \cdot \sigma_{\tilde{N}_j}^{2\cdot\alpha} / \sigma_{C_j}^2 << 1$ для будь-якого значення. Зрозуміло, що за $\alpha = 1$ декомпозиція жодним чином не впливатиме на пропускну здатність стеганоканалу. За $\alpha < 1$ пропускна здатність буде зростати за рахунок того, що в області з низькою дисперсією (високочастотній області) до стеганосигналу додається відносно більше енергії.

Відомо, що перетворення можна впорядкувати за досяжними виграшами від алгоритму кодування (рис. 3.4).

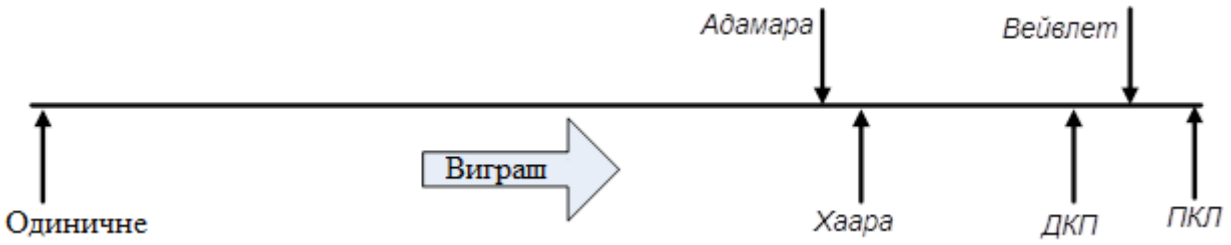


Рис. 3.4. Види перетворень, впорядковані за досяжними виграшами від використання

Під виграшем від кодування мається на увазі ступінь перерозподілу дисперсій коефіцієнтів перетворення. Найбільший виграш дає перетворення Карунена-Лоєва (ПКЛ), найменший – розкладання за базисом одиничного імпульсу (тобто відсутність перетворення).

Перетворення, які відзначаються високими значеннями виграшу від кодування, такі як ДКП, вейвлет-перетворення, характеризуються різко нерівномірним розподілом дисперсій коефіцієнтів субсмуг. Високочастотні субсмуги не підходять для вбудовування через значний шум обробки, а низькочастотні – через значний шум зображення (див. рис. 3.3). Тому доводиться обмежуватися середньочастотними смугами, у яких шум зображення приблизно дорівнює шуму обробки. Оскільки таких смуг мала кількість, то пропускна здатність стеганоканалу є порівняно малою.

У разі застосування перетворення з більш низьким виграшем від кодування, наприклад перетворення Адамара або Фур'є, існує більше блоків, у яких шум зображення приблизно дорівнює шуму обробки, отже, і пропускна здатність вище. Тобто для підвищення пропускної здатності стеганографічного каналу доцільно застосовувати перетворення з меншими виграшами від кодування, які погано підходять для компресії сигналів.

Ефективність застосування вейвлет-перетворення і ДКП для компресії зображень пояснюється тим, що вони добре моделюють процес обробки зображення в ЗСЛ, відділяючи суттєві деталі від другорядних. Таким чином, ці перетворення більш доцільно використовувати в випадках присутності активного порушника, оскільки модифікація значущих коефіцієнтів може призвести до неприйнятного спотворення зображення.

Під час застосування перетворень з низькими значеннями виграшу від кодування існує значна небезпека руйнування вбудованих даних у зв'язку з тим, що коефіцієнти перетворення менш стійкі до модифікацій. Однак при цьому існує велика гнучкість у виборі перетворення, і якщо останнє невідомо порушнику, то модифікувати стеганограму буде істотно складніше.

Під час цифрової обробки зображення часто застосовується двовимірна версія дискретного косинусного перетворення:

$$\Omega(\upsilon,\nu)=\frac{\xi(\upsilon)\cdot\xi(\nu)}{\sqrt{2\mathrm{N}}}\cdot\sum_{\mathrm{x}=0}^{\mathrm{N}-1}\sum_{\mathrm{y}=0}^{\mathrm{N}-1}\mathrm{C}(\mathrm{x},\mathrm{y})\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2\mathrm{x}+1)}{2\mathrm{N}}\right]\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2\mathrm{y}+1)}{2\mathrm{N}}\right];$$

$$S(x,y)=\frac{1}{\sqrt{2N}}\cdot\sum_{\upsilon=0}^{N-1}\sum_{\upsilon=0}^{N-1}\xi(\upsilon)\cdot\xi(\nu)\cdot\Omega(\upsilon,\nu)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2y+1)}{2N}\right], \quad (3.2)$$

де C(c,y) і S(x,y) – відповідно елементи оригінального і відновленого за коефіцієнтами ДКП зображення розмірністю $\mathrm{N}\times\mathrm{N}$; x, y – просторові координати пікселів зображення; $\Omega(\upsilon,\nu)$ – масив коефіцієнтів ДКП; υ,ν – координати в частотній області; $\xi(\upsilon)=1/\sqrt{2}$, якщо $\upsilon=0$, і $\xi(\upsilon)=1$, якщо $\upsilon>0$.

Розглянемо існуючі методи, які базуються на алгоритмі ДКП.

3.2. Метод відносної заміни величин коефіцієнтів ДКП (метод Е. Коха і Ж. Жао)

Один з найбільш поширених на сьогодні методів приховування конфіденційної інформації в частотній області зображення полягає у відносній заміні величин коефіцієнтів ДКП, який свого часу описали Е. Кох (E. Koch) і Ж. Жао (J. Zhao).

На початковому етапі первинне зображення розбивається на блоки розміром 8x8 пікселів. ДКП застосовується до кожного блоку – формула (3.2), в результаті чого отримують матриці 8x8 коефіцієнтів ДКП, які часто позначають $\Omega_b(\upsilon,\nu)$, де b – номер блоку контейнера C, а (υ,ν) – позиція коефіцієнта в цьому блоці. Кожен блок при цьому призначений для приховування одного біта даних.

Було запропоновано дві реалізації алгоритму: псевдовипадково можуть обиратися два або три коефіцієнти ДКП. Розглянемо перший варіант.

Під час організації секретного каналу абоненти повинні попередньо домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які будуть використовуватися для приховування даних. Задамо ці коефіцієнти їх координатами в масивах коефіцієнтів ДКП: (υ_1,ν_1) і (υ_2,ν_2). Крім цього, зазначені коефіцієнти повинні відповідати косинус-функції з середніми частотами, що забезпечить прихованість інформації в істотних для ЗСЛ областях сигналу, до того ж інформація не буде спотворюватися під час JPEG-компресії з малим коефіцієнтом стиснення.

Безпосередньо процес приховування починається з випадкового вибору блоку C_b зображення, призначеного для кодування b-го біта повідомлення. Вбудовування інформації здійснюється таким чином: для передачі біта «0» прагнуть, щоб різниця абсолютних значень коефіцієнтів ДКП перевищувала деяку позитивну величину, а для передачі біта «1» ця різниця робиться меншою порівняно з деякою від'ємною величиною:

$$\begin{cases} \left|\Omega_b\left(\upsilon_1,\nu_1\right)\right| - \left|\Omega_b\left(\upsilon_2,\nu_2\right)\right| > P, \; при \; m_b = 0; \\ \left|\Omega_b\left(\upsilon_1,\nu_1\right)\right| - \left|\Omega_b\left(\upsilon_2,\nu_2\right)\right| < -P, \; при \; m_b = 1. \end{cases} \tag{3.3}$$

Таким чином, первинне зображення спотворюється за рахунок внесення змін до коефіцієнтів ДКП, якщо їх відносна величина не відповідає приховуваному біту. Чим більше значення P, тим стеганосистема, створена на основі цього методу, є більш стійкою до компресії, однак якість зображення при цьому значно погіршується.

Після відповідного внесення корекції в значення коефіцієнтів, які повинні задовольняти нерівності (3.3), проводиться зворотне ДКП.

Для вилучення даних у декодері виконується аналогічна процедура вибору коефіцієнтів, а рішення про переданий біт приймається за наступним правилом:

$$\begin{cases} m_b^* = 0, \quad при \left|\Omega_b^*\left(\upsilon_1, \nu_1\right)\right| > \left|\Omega_b\left(\upsilon_2, \nu_2\right)\right| \\ m_b^* = 1, \quad при \left|\Omega_b^*\left(\upsilon_1, \nu_1\right)\right| < \left|\Omega_b\left(\upsilon_2, \nu_2\right)\right| \end{cases} \tag{3.4}$$

3.3. Метод Бенгама–Мемона–Ео–Юнг

Д. Бенгам (D. Benham), Н. Мемон (N. Memon), Б.-Л. Ео (B.-L. Yeo) і М. Юнг (M. Yeung) запропонували оптимізовану версію вищерозглянутого методу. Причому оптимізацію було проведено за двома напрямками: по-перше, було запропоновано для вбудовування використовувати не всі блоки, а тільки найбільш підходящі для цього, по-друге, в частотній області блоку для вбудовування вибираються не два, а три коефіцієнти ДКП, що істотно зменшує візуальні спотворення контейнера. Розглянемо зазначені удосконалення більш докладно.

Придатними для вбудовування інформації вважаються такі блоки зображення, які одночасно задовольняють наступним вимогам:

- блоки не повинні мати різких переходів яскравості;
- блоки не повинні бути занадто монохромними.

Блоки, які не відповідають першій вимозі, характеризуються наявністю надто великих значень низькочастотних коефіцієнтів ДКП, що їх за розмірами можна порвіняти з DC-коефіцієнтом. Для блоків, які не задовольняють другій вимозі, характерна рівність нулю більшості високочастотних коефіцієнтів. Зазначені особливості є критерієм відбракування непридатних блоків.

Зазначені вимоги відбракування враховуються використанням двох порогових коефіцієнтів: $\mathbf{P_L}$ (для першої вимоги) і $\mathbf{P_H}$ (для другої вимоги), перевищення ($\mathbf{P_L}$) або недосягнення ($\mathbf{P_H}$) яких буде вказувати на те, що цей блок є непридатним для модифікації в частотній області.

Вбудовування в блок біта повідомлення відбувається наступним чином. Вибираються (для більшої стійкості стеганосистеми – псевдовипадково) три коефіцієнти ДКП блоку з середньочастотної області з координатами (υ_1, ν_1), (υ_2, ν_2) і (υ_3, ν_3). Якщо необхідно провести вбудовування «0», ці коефіцієнти змінюються таким чином (якщо, звичайно, це необхідно), аби третій коефіцієнт став меншим за будь-який з перших двох; якщо необхідно приховати «1», він стає великим порівняно з першим і другим коефіцієнтами:

$$\begin{cases} \left.\begin{aligned} &\left|\Omega_b\left(\upsilon_3, \nu_3\right)\right| < \left|\Omega_b\left(\upsilon_1, \nu_1\right)\right|; \\ &\left|\Omega_b\left(\upsilon_3, \nu_3\right)\right| < \left|\Omega_b\left(\upsilon_2, \nu_2\right)\right| \end{aligned}\right\}, \text{ за } m_b = 0; \\ \left.\begin{aligned} &\left|\Omega_b\left(\upsilon_3, \nu_3\right)\right| > \left|\Omega_b\left(\upsilon_1, \nu_1\right)\right| \\ &\left|\Omega_b\left(\upsilon_3, \nu_3\right)\right| > \left|\Omega_b\left(\upsilon_2, \nu_2\right)\right| \end{aligned}\right\}, \text{ за } m_b = 1. \end{cases} \tag{3.5}$$

Як і в попередньому методі, для прийняття рішення про достатність розрізнення зазначених коефіцієнтів ДКП до виразу (3.5) вводиться значення порогу розрізнення P:

$$\begin{cases} \left|\Omega_b\left(\upsilon_3,\nu_3\right)\right| < \min\left|\Omega_b\left(\upsilon_1,\nu_1\right)\right|,\left|\Omega_b\left(\upsilon_2,\nu_2\right)\right| \ ) - P, \text{за } m_b = 0; \\ \left|\Omega_b\left(\upsilon_3,\nu_3\right)\right| > \max\left|\Omega_b\left(\upsilon_1,\nu_1\right)\right|,\left|\Omega_b\left(\upsilon_2,\nu_2\right)\right| \ ) + P, \text{за } m_b = 1. \end{cases} \quad (3.6)$$

І тому, коли така модифікація призводить до занадто великої деградації зображення, коефіцієнти не змінюють, і блок у якості контейнера не використовується.

Використання трьох коефіцієнтів замість двох і, що найголовніше, відмова від модифікації блоків зображення в разі неприйнятних спотворень зменшує похибки, що вносяться повідомленням. Одержувач завжди може визначити блоки, до яких не проводилося вбудовування, просто повторивши аналіз, аналогічний виконаному на передавальній стороні.

3.4. Метод Дж. Фрідріх

Алгоритм, запропонований Джесікою Фрідріх (J. Fridrich), по суті є комбінацією двох алгоритмів: відповідно до одного з них приховувані дані вбудовуються в низькочастотні, а до іншого – в середньочастотні коефіцієнти ДКП. Каскадне використання двох різних алгоритмів дозволяє отримати хороші результати щодо стійкості стеганографічної системи до атак.

Зображення, яке планується використовувати в якості контейнера, конвертується в сигнал із нульовим математичним очікуванням і певним стандартним відхиленням таким чином, щоб НЧ-коефіцієнти ДКП, які будуть обчислені в подальшому, потрапляли до попередньо заданого незмінного діапазону. Запропоноване перетворення

$$\mathrm{G} = \frac{1024}{\sqrt{\mathrm{X}\cdot\mathrm{Y}}}\cdot\frac{\mathrm{C}-\overline{\mathrm{C}}}{\sigma(\mathrm{C})}, \quad (3.7)$$

де X, Y – розмірність зображення C в пікселях; $\overline{\mathrm{C}}$ і $\sigma(\mathrm{C})$ – відповідно, математичне очікування і стандартне відхилення значень яскравості пікселів зображення, – трансформує напівтонове зображення C у двовимірний сигнал G з нульовим математичним очікуванням. В цьому випадку абсолютне значення максимального НЧ-коефіцієнта ДКП сигналу G не буде перевищувати поріг (200 ... 250). Крім того, стверджується, що це перетворення можна застосувати для широкого кола різноманітних зображень: як із великими однорідними областями, так і сильно текстурованих.

Для сигналу-зображення G проводиться обчислення коефіцієнтів ДКП, з усієї множини яких модифікуються тільки низькочастотні. Причому модифікування проводиться таким чином, щоб в коефіцієнтах було закодовано приховуване повідомлення W, що представляє собою сигнал у вигляді послідовності чисел {-1,1}. Для цього попередньо необхідно визначити геометричну прогресію дійсних чисел

$$\tau_{i+1} = \frac{1+\alpha}{1-\alpha} \cdot \tau_i; \quad \tau_1 = 1, \tag{3.8}$$

параметризованих (що налаштовуються) за допомогою параметра $\alpha \in (0,1)$.

Для значень $t > 1, \tau_i \le t < \tau_{i+1}$ визначається індексна функція

$$\text{ind}(t) = (-1)^i, \text{ если } t \in [\tau_i, \tau_{i+1}), \tag{3.9}$$

що дозволяє для кожного дійсного числа $t > 1$ визначити його індекс (+ / -1). Зрозуміло, що зазначений індекс може бути змінений шляхом додавання або ж віднімання числа, що не перевищує значення $\alpha \cdot t$. На рис. 3.5 наведени індексні функції для $\alpha = 0.1, 0.2$ *та* 0.3.

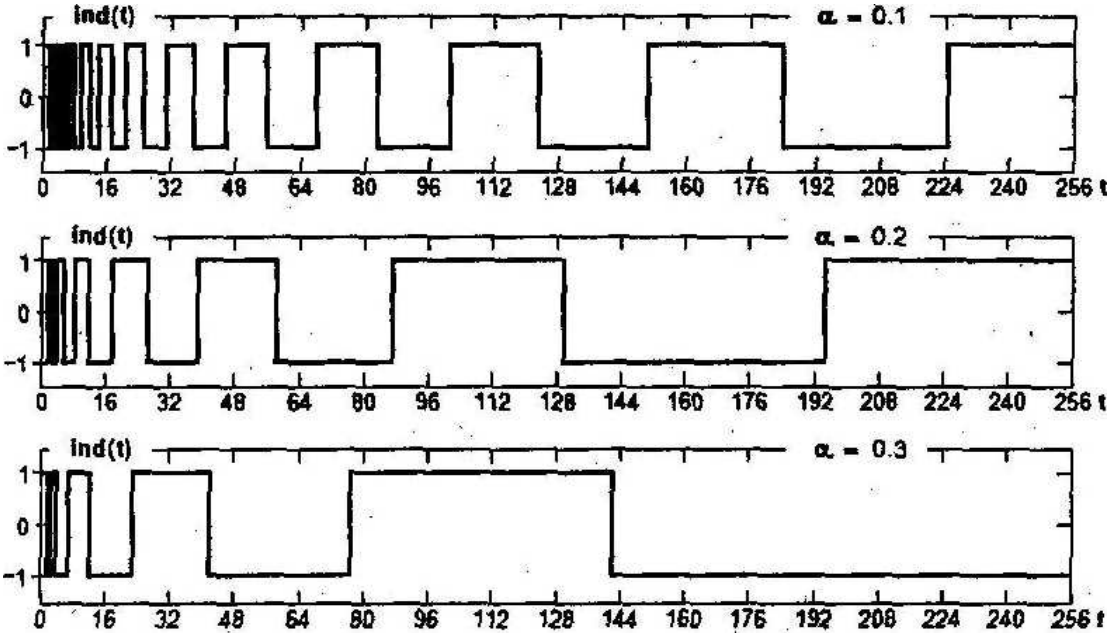


Рис. 3.5. Індексна функція ***Ind(t)*** *за значень* $\alpha = 0.1, 0.2$ *та* 0.3

Для вбудовування масиву повідомлення W, кожен окремий біт якого може приймати значення $W_j \in \{-1, 1\}$, за $j \in \{1, 2, \ldots, \aleph_W\}$, вибираються $\aleph_{\Omega low} = \aleph_W$ НЧ-коефіцієнтів ДКП – Ω_j, значення яких змінюються таким чином, щоб виконувалася умова $\text{ind}(|\Omega^{\Lambda}_j|) = W_j$, де Ω^{Λ}_j – модифіковане значення коефіцієнта ДКП. У тому випадку $|\Omega_j| < 1$, якщо коефіцієнт для

вбудовування не використовується. Завдяки властивостям індексної функції кожен коефіцієнт буде змінений не більше ніж на $100 \cdot \alpha$ відсотків. Також зазначається, що зміни носитимуть випадкових характер, оскільки не існує жодних підстав вважати, що коефіцієнти ДКП на початковому етапі кодування є наслідком певного повідомлення.

Найбільша стійкість стеганосистеми до спотворень контейнера досягається встановленням в якості нових значень коефіцієнтів ДКП середини інтервалів $[\tau_i, \tau_{i+1})$. Однак це може послужити появі скупчень однакових коефіцієнтів ДКП, що робить систему ненадійною з точки зору можливого стеганографічного аналізу. Значення параметру вибирається таким чином, щоб вбудовування повідомлення не призводило до помітних для ока спотворень контейнера.

Операція вилучення проводиться шляхом виконання аналогічних з операцією вбудовування перетворень контейнера, який підозрюється на наявність прихованого повідомлення:

- конвертація в сигнал із нульовим математичним очікуванням за формулою (3.7);
- обчислення коефіцієнтів ДКП конвертованого зображення;
- обчислення для заздалегідь обумовлених коефіцієнтів ДКП індексної функції (3.9) за заданого параметра α;
- формування з отриманих індексів масиву витягнутого повідомлення.

Крім того, Дж. Фрідріх запропонувала метод детектування наявності/відсутності вбудованого повідомлення в контейнері, що може бути корисним під час захисту цифрового контенту (інформаційного вмісту) за допомогою цифрових водяних знаків. Ця операція передбачає обізнаність одержувача щодо змісту прихованого повідомлення.

У зв'язку з тим, що більшість з $\aleph_{\Omega low}$ НЧ-коефіцієнтів було піддано модифікації під час кодування, просте обчислення кореляції між W_i та $ind\left(\left|\Omega^{\wedge}{}_j\right|\right)$ зумовлювало б собою нестійкість методу, оскільки малі, візуально незначні коефіцієнти ДКП роблять такий же ваговий внесок до загальної енергії сигналу, як і великі, візуально більш значущі коефіцієнти.

Оскільки попередньо було висунуто умову, що контейнер з вбудованим повідомленням не повинен привертати увагу, ми не можемо вбудовувати дані тільки в коефіцієнти, що мають велике значення. Крім того, позиції найбільших коефіцієнтів ДКП первинного і модифікованого зображень можуть не збігатися, що унеможливить безпомилкову ідентифікацію тих із них, в які було зроблено вбудовування. У запропонованій автором системі вбудовування здійснюється в усі НЧ-коефіцієнти, незалежно від їх значення (звичайно, крім тих, які не перевищують одиниці),

проте тільки найбільші з них враховуються згодом під час обчислення коефіцієнта кореляції, що зважується з енергією абсолютних значень коефіцієнтів ДКП:

$$K = \frac{\sum_{j=1}^{\aleph_{\Omega low}} \left|\Omega^*_j\right|^\beta \cdot \mathrm{ind}\left(\left|\Omega^*_j\right|\right) W_j}{\sum_{j=1}^{\aleph_{\Omega low}} \left|\Omega^*_j\right|^\beta}. \qquad (3.10)$$

Таке зважування автоматично робить більш виразними найбільші значення коефіцієнтів, одночасно пригнічуючи незначні, які могли зазнати змін у результаті будь-яких операцій з обробки зображення. Параметр встановлює важливість зважування. Якщо $\beta = 0$, то обчислюється звичайний, незважений коефіцієнт кореляції. Значення β, яке є близьким до одиниці, призводить до сингулярності (виродження) системи детектування: функція виявлення буде залежати тільки від значення всього лише одного біта, що відповідає найбільшому коефіцієнту ДКП. Автор методу рекомендує використовувати значення $\beta \in (0.5,1)$.

Більш стійкою до атак цю систему можна зробити шляхом пошуку максимального значення коефіцієнта кореляції щодо стандартного відхилення значень яскравості пікселів зображення, підозрюваного на присутність вбудованого повідомлення.

Масштабування (3.7) залежить від стандартного відхилення значень яскравості пікселів, яке може бути суттєво спотворено, якщо зображення з вбудованим повідомленням було піддано згладжуванню або, наприклад, додатково зашумлено. Як наслідок, коефіцієнти ДКП такого зображення будуть промасштабовані за допомогою фіксованого коефіцієнта (відношення стандартних відхилень оригінального і досліджуваного на наявність прихованого повідомлення зображень $d = \sigma(C)/\sigma(S)$). Однак повідомлення, закодованого в коефіцієнтах ДКП, лінійні зміни не торкнуться. Це робить доцільним використання простого одновимірного пошуку правильного масштабу d, який би максимізував значення коефіцієнта кореляції (оскільки первинне зображення, що використовується в якості контейнера, в детекторі відсутнє). Таким чином, доповнена функція детектування має наступний вигляд:

$$K' = \max_{d \in (1-\delta, 1+\delta)} K(d) \frac{\sum_{j=1}^{\aleph_{\Omega low}} \left|\Omega^*_j\right|^\beta \cdot \mathrm{ind}\left(\left|\Omega^*_j\right|\right) W_j}{\sum_{j=1}^{\aleph_{\Omega low}} \left|\Omega^*_j\right|^\beta}. \qquad (3.11)$$

Встановлено, що навіть за значних спотворень зображення в результаті атак достатнім буде крок відхилення масштабу $\delta = 0{,}25$.

Труднощі детектування, що виникають при цьому, вимагають зменшення інформаційного змісту повідомлення і додавання коригувальних бітів. Отже, оскільки внесок у виявлення повідомлення вносять тільки найбільші коефіцієнти ДКП, інформаційний зміст повідомлення довжиною $\aleph_W$ є лише певною часткою від $\aleph_W$. Крім того, цілком очевидно, що одновимірний пошук масштабного коефіцієнта, який максимізує коефіцієнт кореляції, збільшує відсоток помилкових виявлень.

Для досягнення властивостей високої стійкості до атак на стеганосистему за одночасного мінімального (наскільки, звичайно, це можливо) спотворення контейнера Дж. Фрідріх було запропоновано вмонтувати у контейнер додаткове повідомлення, використовуючи методику розширення спектра. При цьому вбудовування повідомлення здійснюється шляхом додавання шумоподібного сигналу до СЧ-коефіцієнтів ДКП зображення. Кількість таких коефіцієнтів $(\aleph_{\Omega mid})$ складає приблизно 30 % від загальної кількості коефіцієнтів ДКП.

Вважається, що інформація, яку несе додаткове повідомлення, складається з $\aleph_{W^+}$ символів W_j^+, кожен із яких може бути представлений десятковим цілим числом, $1 \le W_j^+ \le \max\left(W^+\right)$.

Для кожного j-го символу генерується послідовність $\xi^{(j)}$ ПВЧ, рівномірно розподілених в інтервалі [0,1]. Початковий стан генератора ПВЧ може виступати в ролі секретного ключа. Потужність j-ї множини ПВЧ: $\left|\xi^{(j)}\right| \ge \aleph_{\Omega mid} + \max\left(W^+\right)$.

Для подання окремого символу повідомлення W^+ з множини $\xi^{(j)}$ виділяється сегмент $\eta^{|j|} = \xi^{(j)}_{W_j^+}, \ldots \xi^{(j)}_{W_j^+ + \aleph_{\Omega mid}-1}$, який містить $\aleph_{\Omega mid}$ елементів.

В результаті повідомлення із $\aleph_{W^+}$ символів може бути представлено у наступному вигляді:

$$Spr = \frac{\left[\sum_{j=1}^{\aleph_{W^+}} \eta^{(j)}\right] - \frac{\aleph_{W^+}}{2}}{\sqrt{\aleph_{W^+}/12}}. \qquad (3.12)$$

Сигнал із розширеним спектром Spr характеризується приблизно нормальним (гаусовим) розподілом із нульовим математичним очікуванням і одиничним стандартним відхиленням (точність апроксимації зростає зі збільшенням значення $\aleph_{W^+}$). Надалі сигнал Spr множиться на параметр γ, який регулює відношення «стійкість/помітність вбудовування» і поелементно підсумовується з $\aleph_{\Omega mid}$ вибраними СЧ-коефіцієнтами. Вилучення

повідомлення виконується шляхом попереднього обчислення коефіцієнтів ДКП зображення і виділення серед них саме середньочастотних (ця операція повинна бути узгодженою з відповідною дією на етапі вбудовування). Використовуючи секретний ключ/алгоритм, здійснюється генерація послідовностей ПВЧ (загальною кількістю $\aleph_{W^+}$, якщо цей параметр відомий; в іншому випадку – за обставинами, виходячи з аналізу вже отриманої частини повідомлення) довжиною $\aleph_{\Omega mid} + \max\left(W^+\right)$.

З кожної послідовності $\xi^{(j)}$ виділяється $\max\left(W^+\right)$ сегментів довжиною $\aleph_{\Omega\,mid}$ елементів, для яких розраховується взаємна кореляція з вектором виділених СЧ-коефіцієнтів. Позиція найбільшого значення функції кореляції в отриманому при цьому векторі і буде визначати значення, яке ймовірно мав вбудований символ W^+_j.

Збільшення параметрів α і, особливо, γ робить цю стеганосистему ще більш стійкою до атаки компресією, однак при цьому сильно страждає якість зображення.

4. ПИТАННЯ ДЛЯ ПОТОЧНОГО КОНТРОЛЮ ПІДГОТОВЛЕНОСТІ СТУДЕНТІВ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ

1. Основні етапи алгоритму стиску зображень JPEG. Які етапи алгоритму JPEG призводять до стиску зображення?

2. Дискретно-косинусне перетворення. Основні співвідношення та властивості.

3. Метод приховування даних у частотну область нерухомих зображень шляхом кодування різниці абсолютних значень коефіцієнтів дискретно-косинусного перетворення (метод Коха–Жао).

4. Метод приховування даних у частотну область нерухомих зображень шляхом кодування декількох різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення (удосконалений метод Коха–Жао – метод Бенгама–Мемона–Ео–Юнг).

5. Метод приховування цифрових водяних знаків у частотну область нерухомих зображень Хсу-Ву. В чому перевага цього методу порівняно із методом Коха–Жао?

6. Приховування та вилучення інформаційних даних у частотну область нерухомих зображень методом Джесіки Фрідріх. Переваги та недоліки методу.

5. ІНСТРУКЦІЯ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ

Завдання 1. Реалізація алгоритмів прямого та зворотного дискретно-косинусного перетворення. Дослідження ефекту частотної чутливості зорової системи людини

1.1. Завантажуємо вихідні дані: контейнер – нерухоме зображення (в форматі *.bmp24); інформаційне повідомлення – текстовий документ (у форматі *.txt). Для цього в середовищі MathCAD виконуємо дії, аналогічні описаним в п. 1.1. інструкції до лабораторної роботи № 1.

1.2. Перетворюємо масив інформаційних даних. Для цього в середовищі MathCAD виконуємо дії, аналогічні описаним в п. 1.2. інструкції до лабораторної роботи № 1.

1.3. Реалізуємо алгоритми прямого та зворотного дискретно-косинусного перетворення. Для цього в середовищі MathCAD виконуємо послідовність перетворень, представлених на рис. 5.1.

$$N := 8 \quad P := 1$$

$$C := \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \left| \begin{array}{l} C_i \leftarrow \frac{1}{\sqrt{2}} \text{ if } i = 0 \\ C_i \leftarrow 1 \text{ if } i > 0 \end{array} \right. \\ C \end{array} \right. \qquad C = \begin{pmatrix} 0.707 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$T(V) := \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \text{for } j \in 0..N-1 \\ \quad\quad T_{i,j} \leftarrow \text{round}\left[\frac{2}{N} \cdot C_i C_j \cdot \frac{1}{P} \cdot \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \left[V_{x,y} \cdot \cos\left[\frac{(2x+1) \cdot i \cdot \pi}{2N} \right] \cdot \cos\left[\frac{(2y+1) \cdot j \cdot \pi}{2N} \right] \right] \right] \\ T \end{array} \right.$$

$$V(T) := \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \text{for } j \in 0..N-1 \\ \quad\quad V_{i,j} \leftarrow \text{round}\left[\sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \left[T_{x,y} \cdot P \cdot \frac{2}{N} \cdot C_x C_y \cdot \cos\left[\frac{(2i+1) \cdot x \cdot \pi}{2N} \right] \cdot \cos\left[\frac{(2j+1) \cdot y \cdot \pi}{2N} \right] \right] \right] \\ V \end{array} \right.$$

Рис. 5.1. Реалізація дискретно-косинусного перетворення в середовищі символьної математики MathCAD

На рис. 5.1 наведені наступні елементи.

Змінна N задає розмір матриці, над якою виконується перетворення, змінна P задає величину порога загрублення. Якщо P = 1, тоді загрублення не проводиться. Використовуємо значення N = 8, тому що такий параметр використовує алгоритм стиснення JPEG.

Змінна C містить службовий масив даних із восьми елементів, необхідних для коректного обчислення дискретно-косинусного перетворення.

Функція T(V) реалізує пряме дискретно-косинусне перетворення масиву V з NxN чисел. В якості аргумента функції T(V) використовуються окремі блоки растрових даних у просторовій області.

Функція V(T) реалізує зворотне дискретно-косинусне перетворення масиву T з NxN чисел. В якості аргумента функції V (T) використовуються окремі блоки растрових даних в частотній області. Змінна P задає величину порога загрублення коефіцієнтів дискретно-косинусного перетворення.

1.4. Розіб'ємо вихідне зображення на блоки, розміром NxN пікселів кожен, виконаємо пряме дискретно-косинусне перетворення для кожного блоку зображення. Для цього в середовищі MathCAD виконуємо послідовність перетворень, представлених на рис. 5.2.

$$nn := \frac{cols(R)}{N} \qquad mm := \frac{rows(R)}{N}$$

$$r := \left| \begin{array}{l} \text{for } x \in 0..mm-1 \\ \quad \text{for } y \in 0..nn-1 \\ \quad\quad \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \text{for } j \in 0..N-1 \\ \quad\quad RR_{i,j} \leftarrow R_{i+x\cdot N,\, j+y\cdot 8} \\ r_{x,y} \leftarrow RR \end{array} \right. \\ r \end{array} \right.$$

$$tr := \left| \begin{array}{l} \text{for } i \in 0..mm-1 \\ \quad \text{for } j \in 0..nn-1 \\ \quad\quad tr_{i,j} \leftarrow T\left(r_{i,j}\right) \\ tr \end{array} \right.$$

Рис. 5.2 Розбиття контейнера-зображення на блоки та виконання над ними дискретно-косинусного перетворення

Величини nn і mm задають число блоків, на які розбито зображення. У масиві r будуть міститися блоки зображення розміром NxN пікселів в просторовій області, а в масиві tr будуть зберігатися ті ж блоки, але вже в частотній області, тобто це масиви коефіцієнтів дискретно-косинусного перетворення. Наприклад, для блоку з номерами 1,2 маємо значення, наведені на рис. 5.3.

$$r_{1,2} = \begin{pmatrix} 24 & 24 & 23 & 22 & 21 & 20 & 20 & 20 \\ 23 & 22 & 21 & 21 & 19 & 19 & 18 & 17 \\ 24 & 22 & 20 & 20 & 20 & 19 & 18 & 16 \\ 25 & 23 & 22 & 21 & 21 & 20 & 19 & 18 \\ 24 & 24 & 23 & 22 & 22 & 21 & 20 & 19 \\ 23 & 23 & 23 & 22 & 21 & 21 & 20 & 20 \\ 22 & 22 & 21 & 21 & 20 & 20 & 20 & 19 \\ 24 & 22 & 21 & 21 & 21 & 21 & 20 & 19 \end{pmatrix} \quad tr_{1,2} = \begin{pmatrix} 168 & 13 & 0 & 2 & 0 & 1 & 0 & 0 \\ -1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 4 & -1 & 0 & -3 & -1 & -1 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

Рис. 5.3 Приклад блоків контейнера-зображення в просторовій та частотній області

Значення масиву $r_{1,2}$ (див. рис. 5.3) характеризують величину яскравості (червоного кольору) окремих пікселів зображення, а значення масиву $tr_{1,2}$ характеризують величину окремих коефіцієнтів дискретно-косинусного перетворення, обчислених для блоку $r_{1,2}$. Ліва верхня частина масиву $tr_{1,2}$ відповідає низькочастотній області зображення, саме тут зосереджена основна «енергія» реалістичних зображень, що наочно видно за значеннями масиву $tr_{1,2}$. Права нижня частина відповідає високочастотній області, значення коефіцієнтів дискретно-косинусного перетворення в якій характеризують високочастотну, контрастну частину зображення. Для реалістичних зображень високочастотна область містить низькі за абсолютною величиною значення, що наочно видно на рис. 5.3.

1.5. Для дослідження ефекту частотної чуттєвості зорової системи людини змінимо величини коефіцієнтів дискретно-косинусного перетворення в низькочастотній і високочастотній області зображення. Внесені зміни будемо оцінювати візуально, для чого виконаємо зворотне дискретно-косинусне перетворення над зміненим масивом коефіцієнтів. Для цього, наприклад, виконаємо перетворення, наведені на рис. 5.4.

Суть перетворень, наведених на рис. 5.4, наступна. Для блоку з номерами 7,7 на 30 % збільшений коефіцієнт дискретно-косинусного перетворення з індексом (0,0). З використанням описаної в п. 1.3 функції V(T) для вихідного і зміненого масиву коефіцієнтів виконано зворотне дискретно-косинусне перетворення. Результат зміни яскравості пікселів (в збільшеному масштабі показані два зображення 8x8 пікселів) показує, що внесені спотворення візуально виявляються (загальний фон зображення ліворуч значно темніше зображення праворуч). Таким чином, навіть незначне (в межах 30 %) спотворення низькочастотних коефіцієнтів дискретно-косинусного перетворення призводить до внесення видимих спотворень, загальний фон змінюється, що добре виявляється на око.

$A := tr_{7,7} \quad B := A$

$B_{0,0} := A_{0,0} + \text{floor}\left(0.3 \cdot A_{0,0}\right)$

$$A = \begin{pmatrix} 444 & 11 & 0 & 0 & 0 & 1 & -1 & 1 \\ -32 & 2 & -2 & 2 & 0 & 0 & 1 & 1 \\ -3 & 0 & -2 & 0 & 1 & 1 & 1 & 0 \\ -7 & -2 & 1 & -1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 577 & 11 & 0 & 0 & 0 & 1 & -1 & 1 \\ -32 & 2 & -2 & 2 & 0 & 0 & 1 & 1 \\ -3 & 0 & -2 & 0 & 1 & 1 & 1 & 0 \\ -7 & -2 & 1 & -1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$a := V(A)$ $\qquad b := V(B)$

$$a = \begin{pmatrix} 50 & 48 & 50 & 48 & 49 & 48 & 47 & 45 \\ 54 & 53 & 53 & 53 & 52 & 50 & 49 & 48 \\ 56 & 56 & 54 & 54 & 54 & 53 & 52 & 50 \\ 58 & 58 & 56 & 55 & 55 & 53 & 54 & 53 \\ 58 & 58 & 58 & 56 & 55 & 55 & 55 & 56 \\ 59 & 60 & 59 & 58 & 57 & 56 & 58 & 57 \\ 61 & 60 & 60 & 60 & 59 & 57 & 59 & 59 \\ 63 & 63 & 63 & 63 & 61 & 60 & 60 & 60 \end{pmatrix} \qquad b = \begin{pmatrix} 67 & 64 & 67 & 65 & 66 & 64 & 63 & 62 \\ 71 & 70 & 70 & 70 & 68 & 66 & 65 & 65 \\ 73 & 73 & 71 & 71 & 71 & 70 & 69 & 66 \\ 74 & 75 & 72 & 72 & 72 & 70 & 71 & 69 \\ 75 & 75 & 75 & 73 & 72 & 72 & 72 & 73 \\ 76 & 77 & 75 & 74 & 74 & 73 & 75 & 74 \\ 77 & 77 & 77 & 77 & 76 & 74 & 76 & 75 \\ 80 & 80 & 79 & 80 & 77 & 77 & 77 & 76 \end{pmatrix}$$

Рис. 5.4. Демонстрація ефекту високої частотної чутливості зорової системи людини до незначної зміни низькочастотних коефіцієнтів зображення

Для розглянутого прикладу внесемо також зміни до коефіцієнта дискретно-косинусного перетворення з індексом (7,6). Це високочастотний коефіцієнт і, згідно з теоретичними відомостями, чутливість зорової системи людини до таких змін дуже низька. Збільшимо обраний коефіцієнт

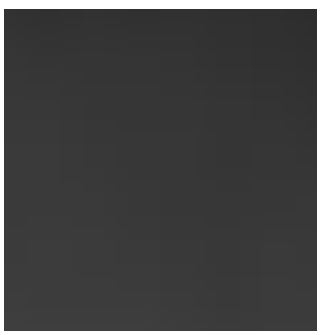
дискретно-косинусного на 100 % і проведемо аналогічні перетворення (див. рис. 5.5). Як видно з наведених даних, навіть після внесення значних змін високочастотного коефіцієнта (збільшення на 100 %), спотворення візуально не виявляються.

$$B_{7,6} := A_{7,6} + \text{floor}\left(A_{7,6}\right)$$

$$A = \begin{pmatrix} 444 & 11 & 0 & 0 & 0 & 1 & -1 & 1 \\ -32 & 2 & -2 & 2 & 0 & 0 & 1 & 1 \\ -3 & 0 & -2 & 0 & 1 & 1 & 1 & 0 \\ -7 & -2 & 1 & -1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 444 & 11 & 0 & 0 & 0 & 1 & -1 & 1 \\ -32 & 2 & -2 & 2 & 0 & 0 & 1 & 1 \\ -3 & 0 & -2 & 0 & 1 & 1 & 1 & 0 \\ -7 & -2 & 1 & -1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}$$

$$a := V(A) \qquad b := V(B)$$

$$a = \begin{pmatrix} 50 & 48 & 50 & 48 & 49 & 48 & 47 & 45 \\ 54 & 53 & 53 & 53 & 52 & 50 & 49 & 48 \\ 56 & 56 & 54 & 54 & 54 & 53 & 52 & 50 \\ 58 & 58 & 56 & 55 & 55 & 53 & 54 & 53 \\ 58 & 58 & 58 & 56 & 55 & 55 & 55 & 56 \\ 59 & 60 & 59 & 58 & 57 & 56 & 58 & 57 \\ 61 & 60 & 60 & 60 & 59 & 57 & 59 & 59 \\ 63 & 63 & 63 & 63 & 61 & 60 & 60 & 60 \end{pmatrix} \qquad b = \begin{pmatrix} 50 & 48 & 50 & 48 & 49 & 48 & 47 & 45 \\ 54 & 53 & 53 & 53 & 52 & 50 & 49 & 48 \\ 56 & 56 & 55 & 54 & 54 & 53 & 52 & 50 \\ 58 & 58 & 56 & 55 & 55 & 53 & 55 & 52 \\ 58 & 58 & 58 & 56 & 55 & 55 & 55 & 56 \\ 59 & 60 & 59 & 58 & 57 & 56 & 58 & 57 \\ 61 & 60 & 60 & 60 & 59 & 57 & 59 & 59 \\ 63 & 63 & 63 & 63 & 61 & 60 & 60 & 60 \end{pmatrix}$$



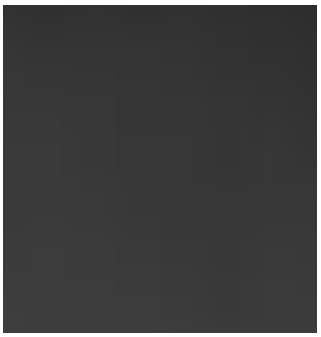


Рис. 5.5. Демонстрація ефекту низької частотної чутливості зорової системи людини до незначної зміни високочастотних коефіцієнтів зображення

Проведемо додаткові дослідження. Посилимо внесені спотворення високочастотного коефіцієнта. Для цього змінимо обраний коефіцієнт на 1000 % і проведемо відповідні перетворення (див. рис. 5.6).

Як видно з наведених на рис. 5.6 даних загальний фон зображення не змінився, проте з'явилися незначні високочастотні спотворення, які за вихідного також візуально не фіксуються.

$$B_{7,6} := A_{7,6} + 10 \cdot \mathrm{floor}\left(A_{7,6}\right)$$

$$A = \begin{pmatrix} 444 & 11 & 0 & 0 & 0 & 1 & -1 & 1 \\ -32 & 2 & -2 & 2 & 0 & 0 & 1 & 1 \\ -3 & 0 & -2 & 0 & 1 & 1 & 1 & 0 \\ -7 & -2 & 1 & -1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 444 & 11 & 0 & 0 & 0 & 1 & -1 & 1 \\ -32 & 2 & -2 & 2 & 0 & 0 & 1 & 1 \\ -3 & 0 & -2 & 0 & 1 & 1 & 1 & 0 \\ -7 & -2 & 1 & -1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 11 & 0 \end{pmatrix}$$

$$a := V(A) \qquad b := V(B)$$

$$a = \begin{pmatrix} 50 & 48 & 50 & 48 & 49 & 48 & 47 & 45 \\ 54 & 53 & 53 & 53 & 52 & 50 & 49 & 48 \\ 56 & 56 & 54 & 54 & 54 & 53 & 52 & 50 \\ 58 & 58 & 56 & 55 & 55 & 53 & 54 & 53 \\ 58 & 58 & 58 & 56 & 55 & 55 & 55 & 56 \\ 59 & 60 & 59 & 58 & 57 & 56 & 58 & 57 \\ 61 & 60 & 60 & 60 & 59 & 57 & 59 & 59 \\ 63 & 63 & 63 & 63 & 61 & 60 & 60 & 60 \end{pmatrix} \qquad b = \begin{pmatrix} 51 & 47 & 50 & 48 & 49 & 48 & 46 & 45 \\ 53 & 54 & 52 & 53 & 52 & 48 & 50 & 48 \\ 57 & 54 & 56 & 53 & 53 & 55 & 50 & 51 \\ 57 & 60 & 54 & 56 & 56 & 51 & 57 & 52 \\ 59 & 56 & 60 & 55 & 54 & 57 & 53 & 57 \\ 59 & 62 & 57 & 58 & 58 & 54 & 60 & 56 \\ 61 & 59 & 61 & 60 & 59 & 59 & 58 & 59 \\ 63 & 64 & 62 & 64 & 61 & 60 & 60 & 59 \end{pmatrix}$$

Рис. 5.6. Демонстрація ефекту низької частотної чутливості зорової системи людини до незначної зміни високочастотних коефіцієнтів зображення

Отже, внесення змін до різних частотних компонентів по-різному впливає на сприйняття цих змін зоровою системою людини: низькочастотні спотворення візуально фіксуються, високочастотні спотворення, як правило, є непомітними. В цьому і проявляється ефект частотної чутливості, який будемо використовувати в подальшому під час реалізації методів стеганографічного вбудовування.

Завдання 2. Реалізація алгоритмів вбудовування та вилучення повідомлень до частотної області зображень (метод Коха–Жао)

2.1. Реалізуємо алгоритм вбудовування інформаційних даних в частотну область зображення на основі кодування різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення. Для цього в середовищі MathCAD виконуємо послідовність перетворень, представлених на рис. 5.7 і 5.8.

$$Pr := 5$$

$$H(H1,H2) := \begin{cases} -1 \\ 1 \text{ if } |H1| - |H2| > Pr \\ 0 \text{ if } |H1| - |H2| < -Pr \end{cases}$$

$$\begin{aligned}
&Input(TRR, m) := \left| \begin{array}{l}
TRR \leftarrow TRR \\
\text{if } m = 1 \wedge m \neq H\left(TRR_{3,1}, TRR_{1,3}\right) \vee H\left(TRR_{3,1}, TRR_{1,3}\right) = -1 \\
\quad \left| \begin{array}{l} TRR_{3,1} \leftarrow \left|TRR_{1,3}\right| + Pr \text{ if } TRR_{3,1} > 0 \\ TRR_{3,1} \leftarrow -\left|TRR_{1,3}\right| - Pr \text{ if } TRR_{3,1} \leq 0 \end{array} \right. \\
\text{if } m = 0 \wedge m \neq H\left(TRR_{3,1}, TRR_{1,3}\right) \vee H\left(TRR_{3,1}, TRR_{1,3}\right) = -1 \\
\quad \left| \begin{array}{l} TRR_{1,3} \leftarrow \left|TRR_{3,1}\right| + Pr \text{ if } TRR_{1,3} > 0 \\ TRR_{1,3} \leftarrow -\left|TRR_{3,1}\right| - Pr \text{ if } TRR_{1,3} \leq 0 \end{array} \right. \\
Input \leftarrow TRR
\end{array} \right.
\end{aligned}$$

Рис. 5.7. Вбудовування одного інформаційного біта в частотну область одного 8x8 блоку зображення

Величина Pr задає поріг зміни частотних коефіцієнтів під час вбудовування інформаційних бітів.

Процедура H (H1, H2) реалізує логічне правило зміни абсолютного значення різниць коефіцієнтів дискретно-косинусного перетворення, позначених змінними H1 і H2:

– якщо перший коефіцієнт за абсолютним значенням більше другого на величину Pr, тоді це відповідає вбудовуванню біта «1»;

– якщо перший коефіцієнт за абсолютним значенням менше другого на величину Pr, тоді це відповідає вбудовуванню біта «0»;

– якщо різниця абсолютних значень коефіцієнтів знаходиться в діапазоні від -Pr до Pr, тоді це відповідає невизначеній ситуації, коли не можна детектувати а ні біт «1», а ні біт «0».

З використанням функції H(H1,H2) в процедурі Input(TRR,m) здійснюється кодування різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення в одному блоці 8x8 коефіцієнтів. Вхідними даними є масив TRR розмірністю 8×8 цілих чисел, а також бітова змінна m, яка передає значення вбудованого біта. В якості змінних обрані коефіцієнти в середньочастотній області з номерами (3,1) і (1,3).

У наступній процедурі tr (див. рис. 5.8) реалізується побітове вбудовування інформації до окремих блоків контейнера за допомогою циклічного виклику процедури Input (TRR, m), де в якості TRR виступає поточний блок контейнера, а в якості m – поточне значення вбудованого біта.

$$
\begin{aligned}
&tr := \left|\begin{array}{l}
num \leftarrow 0 \\
\text{for } x \in 0..mm-1 \\
\quad \text{for } y \in 0..nn-1 \\
\quad\quad \left|\begin{array}{l}
\text{break if } x \cdot nn + y \geq \text{rows}(m) - 1 \\
tr_{x,y} \leftarrow \text{Input}\left(tr_{x,y}, m_{num}\right) \\
num \leftarrow num + 1
\end{array}\right. \\
tr
\end{array}\right. \\
&vr := \left|\begin{array}{l}
\text{for } i \in 0..mm-1 \\
\quad \text{for } j \in 0..nn-1 \\
\quad\quad vr_{i,j} \leftarrow V\left(tr_{i,j}\right) \\
vr
\end{array}\right. \\
&R2 := \left|\begin{array}{l}
\text{for } x \in 0..\text{rows}(vr)-1 \\
\quad \text{for } y \in 0..\text{cols}(vr)-1 \\
\quad\quad \left|\begin{array}{l}
temp1 \leftarrow vr_{x,y} \\
\text{for } i \in 0..N-1 \\
\quad \text{for } j \in 0..N-1 \\
\quad\quad temp2_{x \cdot N+i,\, y \cdot N+j} \leftarrow temp1_{i,j}
\end{array}\right. \\
temp2
\end{array}\right.
\end{aligned}
$$

Рис. 5.8. Побітове вбудовування послідовності інформаційних бітів у частотну область зображення

Процедура vr реалізує послідовне зворотне дискретно-косинусне перетворення над зміненими блоками контейнера. Після чого за допомогою процедури R2 блоки об’єднуються в один масив даних, тобто формується нове зображення в просторовій області з уже вбудованими інформаційними даними.

2.2. Виконаємо зорове порівняння двох зображень – до і після вбудовування інформаційних повідомлень. Для цього скористаємося масивами растрових даних (яскравостей пікселів червоного кольору) R і R2. Масив R містить растрові дані до вбудовування, R2 – масив, отриманий під час виконання попереднього пункту.

Слід зазначити, що отримане зображення R2 може містити некоректні значення, тому що внесення змін до частотної області безпосередньо впливає також на значення в просторовій області. Нові значення в просторовій області можуть бути вище 255 або нижче 0, проте в оброблюваному форматі зображення допустимими значеннями є тільки цілі числа від 0 до 255. Значення 256 середовищем символьної математики буде інтерпретовано як число 0, 257 – як число 2, значення -3 – як число 253 і т. д. Для уникнення такої помилкової інтерпретації даних виконаємо наступну процедуру (див. рис. 5.9), яка округлить всі числа, більші за 255 до 255, а всі числа менші 0 до 0.

$$
\begin{aligned}
R2 := \;& \text{for } i \in 0..\text{rows}(R2) - 1 \\
& \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\
& \qquad R2_{i,j} \leftarrow 0 \text{ if } R2_{i,j} < 0 \\
& \qquad R2_{i,j} \leftarrow 255 \text{ if } R2_{i,j} > 255 \\
& R2
\end{aligned}
$$

R *R2*

Рис. 5.9. Обробка масиву растрових даних (R) та виведення отриманого зображення (R2)

На рис. 5.9 наведено для візуального порівняння два зображення: до вбудовування інформаційних даних (зліва) і після внесених змін (праворуч). Зрозуміло, що візуально наведені зображення не відрізняються.

Для кількісної оцінки відмінностей зображень обчислимо середнє арифметичне поелементної різниці масивів R і R2 (див. рис. 5.10).

Для кількісної оцінки відмінностей зображень обчислимо середнє арифметичне поелементної різниці масивів R та R2 (див. рис. 5.10).

$$
\begin{aligned}
RAZ := \;& RAZ \leftarrow 0 \\
& \text{for } i \in 0..\text{rows}(R2) - 1 \\
& \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\
& \quad\quad RAZ \leftarrow RAZ + \left| R_{i,j} - R2_{i,j} \right| \\
& RAZ \leftarrow \frac{RAZ}{\text{rows}(R)\cdot\text{cols}(R)} \\
& RAZ
\end{aligned}
$$

$$RAZ = 0.974$$

Рис. 5.10. Кількісна оцінка відмінностей між зображеннями до і після вбудовування інформаційного повідомлення

Зрозуміло, що зображення відрізняються досить незначимо, отримана величина усереднених спотворень знаходиться нижче порогу чутливості зорової системи людини, тобто під час візуального огляду спотворення не виявляються.

2.3. Реалізуємо алгоритм вилучення інформаційних даних з частотної області зображення. Для цього в середовищі MathCAD виконаємо послідовність перетворень, представлених на рис. 5.11.

$$
\begin{aligned}
tr1 := \;& \text{for } i \in 0..mm - 1 \\
& \quad \text{for } j \in 0..nn - 1 \\
& \quad\quad tr_{i,j} \leftarrow T\left(vr_{i,j}\right) \\
& tr
\end{aligned}
$$

$$
\begin{aligned}
m1 := \;& num \leftarrow 0 \\
& \text{for } x \in 0..mm - 1 \\
& \quad \text{for } y \in 0..nn - 1 \\
& \quad\quad TRR1 \leftarrow tr1_{x,y} \\
& \quad\quad m1_{num} \leftarrow 1 \text{ if } \left|TRR1_{3,1}\right| > \left|TRR1_{1,3}\right| \\
& \quad\quad m1_{num} \leftarrow 0 \text{ if } \left|TRR1_{3,1}\right| \le \left|TRR1_{1,3}\right| \\
& \quad\quad num \leftarrow num + 1 \\
& m1
\end{aligned}
$$

$m =$

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

$m1 =$

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

Рис. 5.11. Побітовий витяг послідовності інформаційних бітів із частотної області зображення і порівняння даних

У першій процедурі tr1 (див. рис. 5.11) реалізується пряме дискретно-косинусне перетворення всіх блоків контейнера. У наступній процедурі m1 виконується обчислення інформаційних бітів за допомогою вилучення із середньочастотної області масивів коефіцієнтів дискретно-косинусного перетворення. Для цього в кожному блоці порівнюються абсолютні значення коефіцієнтів з номерами (3,1) і (1,3). Якщо абсолютне значення коефіцієнта з номером (3,1) більше за абсолютне значення коефіцієнта з номером за (1,3) – тоді детектується одиничний інформаційний біт. В іншому випадку – детектується нульовий інформаційний біт.

На рис. 5.11 для порівняння наведені також значення масивів інформаційних бітів до вбудовування (зліва) і після вилучення (праворуч). Як видно з наведеного прикладу, перші 15 інформаційних бітів збігаються.

Для кількісної ймовірності помилкового вилучення інформаційних даних виконаємо такі операції (див. рис. 5.12).

$$\begin{aligned}
&Po := \left|\begin{array}{l} Po \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(m1) - 1 \\ \quad Po \leftarrow Po + 1 \text{ if } m_i \neq m1_i \\ Po \leftarrow \dfrac{Po}{\text{rows}(m1)} \\ Po \end{array}\right. \\
&Po = 0
\end{aligned}$$

Рис. 5.12. Оцінка ймовірності помилкового вилучення інформаційних даних

Як видно з отриманих результатів, інформаційні біти, витягнуті з частотної області контейнера-зображення, повністю збіглися з вихідними даними. Це було прогнозовано, адже на заповнений контейнер не здійснювалося жодних впливів.

Завдання 3. Реалізація стеганоатаки на основі використання алгоритму стискання JPEG та дослідження її можливостей

3.1. Для реалізації стеганоатаки спершу збережемо заповнений контейнер-зображення (стеганограму) у вигляді окремого файла. Для цього сформуємо масиви яскравостей зеленого G2 і синього B2 кольору і вико-

наємо відповідну команду «WRITERGB» для запису растрових даних до файла (див. рис. 5.13). В результаті виконання цієї команди в теці з реалізацією алгоритмів буде сформований файл «Stego.bmp».

Для візуального порівняння порожнього і заповненого контейнера виведемо на екран зображення до (зліва) і після (праворуч) вбудовування (см. рис. 5.13).

$$G2 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R2) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\ \quad\quad G2_{i,j} \leftarrow G_{i,j} \\ G2 \end{array} \right. \qquad B2 := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(R2) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\ \quad\quad B2_{i,j} \leftarrow B_{i,j} \\ B2 \end{array} \right.$$

$$\text{WRITERGB}("Stego.bmp") := \text{augment}(R2, G2, B2)$$

"1"

"Stego"

Рис. 5.13. Запис заповненого контейнера-зображення до файла «Stego.bmp» і виведення зображення

3.2. Зімітуємо стеганоатаку на основі використання алгоритму стиснення JPEG. Для цього відкриємо файл «Stego.bmp» зовнішнім графічним редактором, наприклад Adobe Photoshop, Corel PHOTO-PAINT або Microsoft Paint. На рис. 5.14 наведено приклад для випадку використання графічного редактора Corel PHOTO-PAINT. У відкритому редакторі збережемо (експортуємо) зображення у форматі JPEG. При цьому будемо використовувати високу якість[1], прийняту за замовчуванням (див. рис. 5.14).

[1] У графічному редакторі Microsoft Paint можливість вибору якості зображення не передбачена. Під час виконання цього завдання лабораторної роботи слід використовувати ті налаштування графічного редактора, які прийнято за замовчуванням.

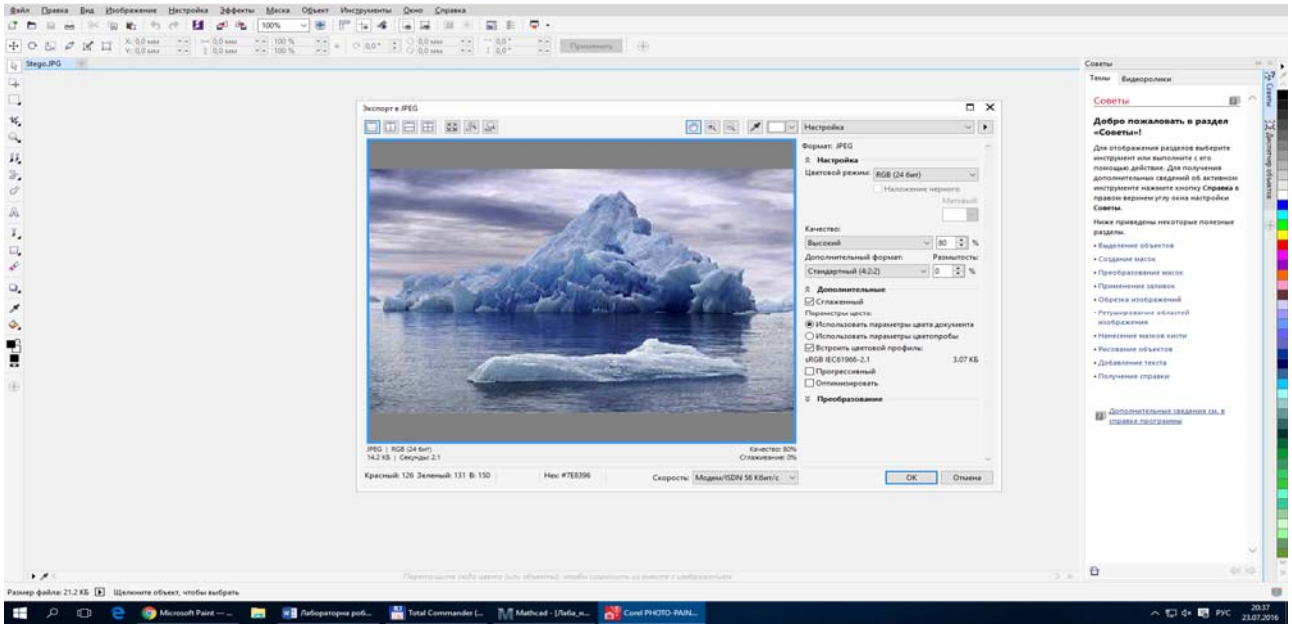


Рис. 5.14. Імітація стеганоатаки на основі алгоритму стиснення JPEG у графічному редакторі Corel PHOTO-PAINT

Отримане в результаті зазначених перетворень зображення буде збережено у форматі JPEG, при цьому інформаційні дані, що містяться в ньому, можуть спотворитися в результаті виконання алгоритму стиснення JPEG.

3.3. Вилучимо вбудовані дані зі стисненого (атакованого) контейнера-зображення. Для цього виконаємо перетворення, наведені на рис. 5.15 (за аналогією з перетвореннями, викладеними в п. 2.3)

```
R_Stego := READ_RED("Stego.jpg")

r2 := | for x ∈ 0..mm − 1
      |   for y ∈ 0..nn − 1
      |     for i ∈ 0..N − 1
      |       for j ∈ 0..N − 1
      |         RR_{i,j} ← R_Stego_{i+x·N, j+y·N}
      |     r_{x,y} ← RR
      | r

tr2 := | for i ∈ 0..mm − 1
       |   for j ∈ 0..nn − 1
       |     tr_{i,j} ← T(r2_{i,j})
       | tr

m1 := | num ← 0
      | for x ∈ 0..mm − 1
      |   for y ∈ 0..nn − 1
      |     TRR1 ← tr2_{x,y}
      |     m1_num ← 1 if |TRR1_{3,1}| > |TRR1_{1,3}|
      |     m1_num ← 0 if |TRR1_{3,1}| ≤ |TRR1_{1,3}|
      |     num ← num + 1
      | m1
```

Рис. 5.15. Побітове вилучення послідовності інформаційних бітів із частотної області стисненого зображення і порівняння даних

Першою командою зчитується масив яскравостей червоного кольору в змінну «R_Stego». Далі цей масив розбивається на блоки розміром NxN елементів, і над кожним блоком за допомогою функції T(V) виконується пряме дискретно-косинусное перетворення. Потім, як і в п. 2.3, виконується послідовне вилучення інформаційних бітів, результат вилучення записується в масив «m1».

3.4. Для кількісної ймовірності помилкового вилучення інформаційних даних виконаємо такі операції (див. рис. 5.16). На рисунку наведено також в якості прикладу перші 15 бітів вбудованих і вилучених зі стисненого контейнера інформаційних даних.

$$Po := \left| \begin{array}{l} Po \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(m1) - 1 \\ \quad Po \leftarrow Po + 1 \text{ if } m_i \neq m1_i \\ Po \leftarrow \dfrac{Po}{\text{rows}(m1)} \\ Po \end{array} \right.$$

$$Po = 0.394$$

$m =$

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

$m1 =$

	0
0	1
1	0
2	0
3	0
4	1
5	0
6	0
7	0
8	1
9	0
10	0
11	1
12	0
13	1
14	1
15	...

Рис. 5.16. Емпірична оцінка ймовірності помилкового вилучення інформаційних даних та порівняння з вихідними даними

Як видно з наведених на рис. 5.16 даних, стиснення зображення призвело до істотного (близько 40 %) спотворення інформаційних бітів. Це наочно підтверджує і наведений на рисунку приклад.

3.5. Зменшимо число виникаючих помилкових даних під час вилучення інформаційних повідомлень. Для цього змінимо параметр «Pr» – величину порога зміни частотних коефіцієнтів під час вбудовування інформаційних бітів (див. п. 2.1). Виберемо значення порога рівним 10 і повторимо всі виконані раніше процедури: вбудовування, збереження зображення у вигляді файла-зображення, стиснення зображення алго-

ритмом JPEG (імітація стеганоатаки) і вилучення повідомлення зі стисненого зображення. Емпірична оцінка ймовірності помилкового вилучення інформаційних даних (див. п. 3.4) дає значення 0,323, тобто кількість помилок зменшилася. Однак збільшення порога «Pr» неминуче призведе до збільшення внесених спотворень до контейнер-зображення. Емпірична оцінка (див. п. 2.2) підтверджує це, отримане значення 1,273 (порівняно з 0,974 за поріг, рівний 5). Повторимо відповідні експериментальні дослідження для різних значень порога «Pr»: 15, 20, 25, 30, 35, 40, 45, 50. Отримані емпіричні оцінки ймовірності помилкового вилучення інформаційних даних та середньої величини внесених спотворень в контейнер-зображення зведемо до відповідних таблиць (див. рис. 5.17).

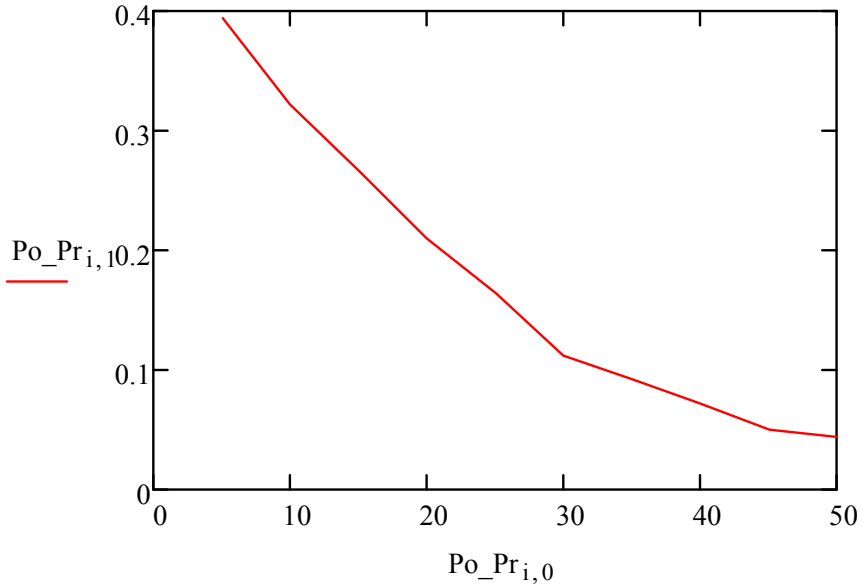
У таблиці «Po_Pr» наведено отримані експериментальні дані в результаті емпіричної оцінки ймовірності помилкового вилучення інформаційних даних (другий стовпець) залежно від величини порога «Pr» (перший стовпець). У таблиці «RAZ_Pr» наведено отримані експериментальні дані в результаті емпіричної оцінки середньої величини внесених спотворень у контейнер-зображення (другий стовпець) залежно від величини порога «Pr» (перший стовпець).

Як видно з наведених на рис. 5.17 залежностей, зі збільшенням величини порога «Pr» ймовірність помилкового вилучення інформаційних бітів повідомлення різко знижується. Однак це веде до аналогічного підвищення внесених спотворень у контейнер-зображення. Якщо використовувати величину порога чутливості зорової системи людини у 2–3 % від максимальної яскравості зображення, тоді внесення спотворень менших за 256*0,02 = 5,12 рівнів яскравості досягається тільки за величини порога «Pr», меншого за 50. Отже, реалізований метод стенографічного вбудовування інформації дозволяє передавати приховані (від візуального виявлення) повідомлення з ймовірністю помилки витягу, не меншою від 0,05. Зниження помилок в інформаційних даних може бути досягнуто за рахунок використання завадостійкого кодування (див. лабораторну роботу № 2) та/або більш надійних методів.

На рис. 5.17 наведені також емпіричні залежності у вигляді графіків, побудованих за відповідними табличними значеннями.

$$Po\_Pr := \begin{pmatrix} 5 & 0.394 \\ 10 & 0.323 \\ 15 & 0.266 \\ 20 & 0.21 \\ 25 & 0.165 \\ 30 & 0.113 \\ 35 & 0.092 \\ 40 & 0.073 \\ 45 & 0.051 \\ 50 & 0.045 \end{pmatrix} \qquad RAZ\_Pr := \begin{pmatrix} 5 & 0.974 \\ 10 & 1.273 \\ 15 & 1.692 \\ 20 & 2.134 \\ 25 & 2.601 \\ 30 & 3.121 \\ 35 & 3.568 \\ 40 & 4.012 \\ 45 & 4.560 \\ 50 & 5.069 \end{pmatrix}$$

$i := 0..9$



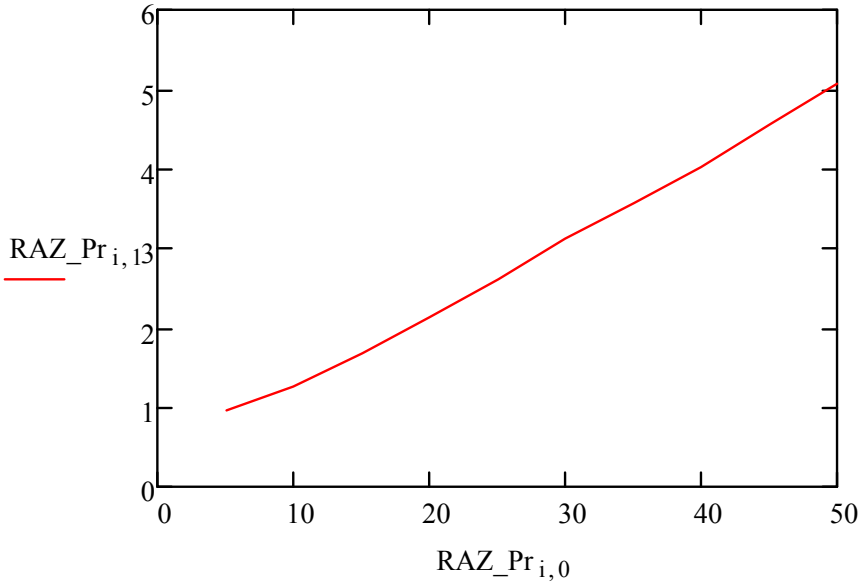


Рис. 5.17. Побудова емпіричних залежностей ймовірності помилкового вилучення інформаційних даних та середньої величини внесених спотворень в контейнер-зображення від величини порога «Pr»

Завдання 4. Реалізація вдосконалених алгоритмів вбудовування та вилучення повідомлень до частотної області зображень (метод Бенгама–Мемона–Ео–Юнг)

4.1. Реалізуємо алгоритм вбудовування інформаційних даних до частотної області зображення на основі вдосконаленого правила кодування різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення (за допомогою методу Бенгама–Мемона–Ео–Юнг). Для цього в середовищі MathCAD виконуємо послідовність перетворень, представлених на рис. 5.18 і 5.19.

$$
\begin{aligned}
&\text{Input}(TRR, m) := \left|\begin{array}{l}
\text{if } m = 1 \\
\quad \left|\begin{array}{l}
TRR_{3,1} \leftarrow \left|TRR_{1,3}\right| + Pr \text{ if } TRR_{3,1} > 0 \\
TRR_{3,1} \leftarrow -\left|TRR_{1,3}\right| - Pr \text{ if } TRR_{3,1} \le 0 \\
TRR_{3,2} \leftarrow \left|TRR_{1,3}\right| + Pr \text{ if } TRR_{3,2} > 0 \\
TRR_{3,2} \leftarrow -\left|TRR_{1,3}\right| - Pr \text{ if } TRR_{3,2} \le 0
\end{array}\right. \\
\text{if } m = 0 \\
\quad \left|\begin{array}{l}
TRR_{1,3} \leftarrow \left|TRR_{3,1}\right| + Pr \text{ if } TRR_{1,3} > 0 \\
TRR_{1,3} \leftarrow -\left|TRR_{3,1}\right| - Pr \text{ if } TRR_{1,3} \le 0 \\
TRR_{2,3} \leftarrow \left|TRR_{3,1}\right| + Pr \text{ if } TRR_{2,3} > 0 \\
TRR_{2,3} \leftarrow -\left|TRR_{3,1}\right| - Pr \text{ if } TRR_{2,3} \le 0
\end{array}\right. \\
TRR
\end{array}\right.
\end{aligned}
$$

Рис. 5.18. Вдосконалене правило кодування різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення

На рис. 5.18 наведено правило кодування різниць абсолютних значень коефіцієнтів, що відповідає першому удосконаленню відповідно до методу Бенгама–Мемона–Ео–Юнг. Замість двох коефіцієнтів дискретно-косинусного перетворення (в методі Коха–Жао) використовується три коефіцієнти і, за твердженням авторів методу, це істотно покращує експлуатаційні характеристики стеганографічного захисту. Друге вдосконалення, засноване на відбракуванні блоків, пропонується реалізувати самостійно.

На рис. 5.19 наведено опис процедур вбудовування даних у контейнер-зображення за допомогою вдосконаленої процедури кодування різниць абсолютних значень коефіцієнтів.

```
tr := | for i ∈ 0..mm − 1
      |   for j ∈ 0..nn − 1
      |     tr_{i,j} ← T(r_{i,j})
      | tr
```

```
tr := | num ← 0
      | for x ∈ 0..mm − 1
      |   for y ∈ 0..nn − 1
      |     | break if x·nn + y ≥ rows(m)
      |     | tr_{x,y} ← Input(tr_{x,y}, m_{num})
      |     | num ← num + 1
      | tr
```

```
vr := | for i ∈ 0..mm − 1
      |   for j ∈ 0..nn − 1
      |     vr_{i,j} ← V(tr_{i,j})
      | vr
```

```
R2 := | for x ∈ 0..rows(vr) − 1
      |   for y ∈ 0..cols(vr) − 1
      |     | temp1 ← vr_{x,y}
      |     | for i ∈ 0..N − 1
      |     |   for j ∈ 0..N − 1
      |     |     temp2_{x·N+i, y·N+j} ← temp1_{i,j}
      | temp2
```

Рис. 5.19. Вбудовування даних у контейнер-зображення за допомогою вдосконаленої процедури кодування різниць абсолютних значень коефіцієнтів дискретно-косинусного перетворення

Перетворення, опис яких наведено на рис. 5.19, аналогічні тим, які розглянуто на рис. 5.8. За аналогією з рис. 5.9 на рис. 5.20 наведено остаточну обробку масиву растрових даних і виведення отриманого зображення.

4.2. Для кількісної оцінки внесених спотворень у контейнер-зображення обчислимо середнє арифметичне поелементної різниці масивів R (до вбудовування) і R2 (після вбудовування). Отримані результати наведено на рис. 5.21.

```
R2 := | for x ∈ 0..rows(vr) − 1
      |   for y ∈ 0..cols(vr) − 1
      |     temp1 ← vr_{x,y}
      |     for i ∈ 0..N − 1
      |       for j ∈ 0..N − 1
      |         temp2_{x·N+i, y·N+j} ← temp1_{i,
      | temp2
```

R *R2*

Рис. 5.20. Обробка масиву растрових даних (R) та виведення отриманого зображення (R2)

$$
\begin{aligned}
RAZ := \;& RAZ \leftarrow 0 \\
& \text{for } i \in 0..\text{rows}(R2) - 1 \\
& \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\
& \quad\quad RAZ \leftarrow RAZ + \left| R_{i,j} - R2_{i,j} \right| \\
& RAZ \leftarrow \frac{RAZ}{\text{rows}(R)\cdot\text{cols}(R)} \\
& RAZ
\end{aligned}
$$

$$RAZ = 1.815$$

Рис. 5.21. Кількісна оцінка різниць між зображеннями до та після вбудовування інформаційного повідомлення

Зрозуміло, що величина внесених спотворень в удосконаленому методі порівняно з методом Коха–Жао істотно (практично в два рази) зросла. Це пояснюється відсутністю процедури відбраковування та вбудовуванням даних у три (замість двох) коефіцієнти дискретно-косинусного перетворення. Однак цей окремий випадок є неінформативним. Необхідно

оцінити також ймовірність помилкового вилучення інформаційних даних, а також дослідити відповідні залежності для різних значень порога «Pr».

4.3. Реалізуємо алгоритм вилучення інформаційних даних із частотної області зображення. Для цього в середовищі MathCAD виконаємо послідовність перетворень, представлених на рис. 5.22 (за аналогією з перетвореннями, представленими на рис. 5.11).

```
tr1 := | for i ∈ 0.. mm − 1
       |   for j ∈ 0.. nn − 1
       |     tr[i,j] ← T(vr[i,j])
       | tr

m1 := | num ← 0
      | for x ∈ 0.. mm − 1
      |   for y ∈ 0.. nn − 1
      |     | TRR1 ← tr1[x,y]
      |     | m1[num] ← 1  if |TRR1[3,1]| > |TRR1[1,3]| ∧ |TRR1[3,2]| > |TRR1[1,
      |     | m1[num] ← 0  if |TRR1[3,1]| ≤ |TRR1[1,3]| ∧ |TRR1[3,2]| ≤ |TRR1[1,
      |     | num ← num + 1
      | m1
```

Рис. 5.22. Побітове вилучення послідовності інформаційних бітів із частотної області зображення і порівняння даних

Після виконання дискретно-косинусного перетворення всіх блоків контейнера (процедура «tr1») проводиться обчислення інформаційних бітів (масив «m1») за допомогою вилучення з середньочастотної області масивів коефіцієнтів дискретно-косинусного перетворення. Для цього в кожному блоці порівнюються абсолютні значення коефіцієнтів із за номерами (3,1), (1,3) і (3,2). Якщо абсолютне значення коефіцієнта з номером (3,1) більше абсолютне значення коефіцієнта з номером (1,3) і одночасно коефіцієнта з номером (3,2), тоді детектується одиничний інформаційний біт. Якщо абсолютне за значення коефіцієнта з номером (3,1) менше або дорівнює абсолютному значенню коефіцієнта з номером (1,3) і одночасно коефіцієнта з номером (3,2), тоді детектується нульовий інформаційний біт.

Для кількісної ймовірності помилкового вилучення інформаційних даних виконаємо операції, наведені на рис. 5.23 (за аналогією з рис. 5.12).

Витягнуті з частотної області контейнера-зображення інформаційні біти повністю збіглися (див. рис. 5.23) з вихідними даними (як і в методі прототипу), що пояснюється відсутністю внесених спотворень у контейнер-зображенні.

$$
\begin{aligned}
&Po := \left| \begin{array}{l} Po \leftarrow 0 \\ \text{for } i \in 0..\,\mathrm{rows}(m1) - 1 \\ \quad Po \leftarrow Po + 1 \text{ if } m_i \neq m1_i \\ Po \leftarrow \dfrac{Po}{\mathrm{rows}(m1)} \\ Po \end{array} \right. \\
&Po = 0
\end{aligned}
$$

Рис. 5.23. Оцінка ймовірності помилкового вилучення інформаційних даних

4.4. Проведемо емпіричні дослідження ефективності вдосконаленого методу стеганографічного перетворення (за аналогією з розглянутим вище завданням 3). Експериментальні дослідження часток внесених спотворень у контейнер-зображення і кількості виникаючих помилок під час вбудовування інформаційних даних проведемо для різних значень порога «Pr»: 15, 20, 25, 30, 35, 40, 45, 50 (як і під час виконання завдання 3). Отримані емпіричні оцінки ймовірності помилкового вилучення інформаційних даних та середньої величини внесених спотворень до контейнер-зображення зведемо до відповідних таблиць, наведених на рис. 5.24 (за аналогією з рис. 5.17).

Таблиці «Po_Pr1» і «RAZ_Pr1» характеризують величину помилок у витягнутих даних і рівень внесених спотворень до контейнер-зображення. Вони заповнені таким же чином, як і відповідні таблиці «Po_Pr» і «RAZ_Pr» на рис. 5.17.

На рис. 5.24 приведено також емпіричні залежності у вигляді графіків, побудованих за відповідними табличними значеннями. На графіках суцільною лінією наведено емпіричні залежності, що характеризують ефективність методу Коха–Жао, переривчастою лінією – дані для вдосконаленого методу. Як видно з наведених залежностей, вдосконалений метод дійсно дозволяє знизити кількість виникаючих помилок під час вбудовування інформаційних даних (перший графік). Однак його використання пов’язане також зі збільшенням внесених спотворень до контейнер-зображення (другий графік). Якщо зафіксувати рівень внесених спотворень у 2–3 % від максимальної яскравості зображення (256*0,02 = 5,12), тоді величина порога «Pr» не повинна перевищувати 40 (див. другий графік). Це приблизно відповідає ймовірності помилки вилучення близько 0,05. Тобто з точки зору величини

внесених спотворень і помилок, що виникають під час вбудовування інформаційних даних, метод Коха–Жао і вдосконалений метод (метод Бенгама–Мемон–Ео–Юнг) можна порівняти за ефективністю. Це пояснюється а відсутністю процедури відбракування блоків в удосконаленому методі (цю процедуру пропонується реалізувати самостійно).

$$Po\_Pr1 := \begin{pmatrix} 5 & 0.391 \\ 10 & 0.275 \\ 15 & 0.221 \\ 20 & 0.173 \\ 25 & 0.142 \\ 30 & 0.099 \\ 35 & 0.081 \\ 40 & 0.055 \\ 45 & 0.042 \\ 50 & 0.038 \end{pmatrix} \qquad RAZ\_Pr1 := \begin{pmatrix} 5 & 1.815 \\ 10 & 2.273 \\ 15 & 2.692 \\ 20 & 3.142 \\ 25 & 3.351 \\ 30 & 3.721 \\ 35 & 4.298 \\ 40 & 5.431 \\ 45 & 6.169 \\ 50 & 6.801 \end{pmatrix}$$

$i := 0..9$

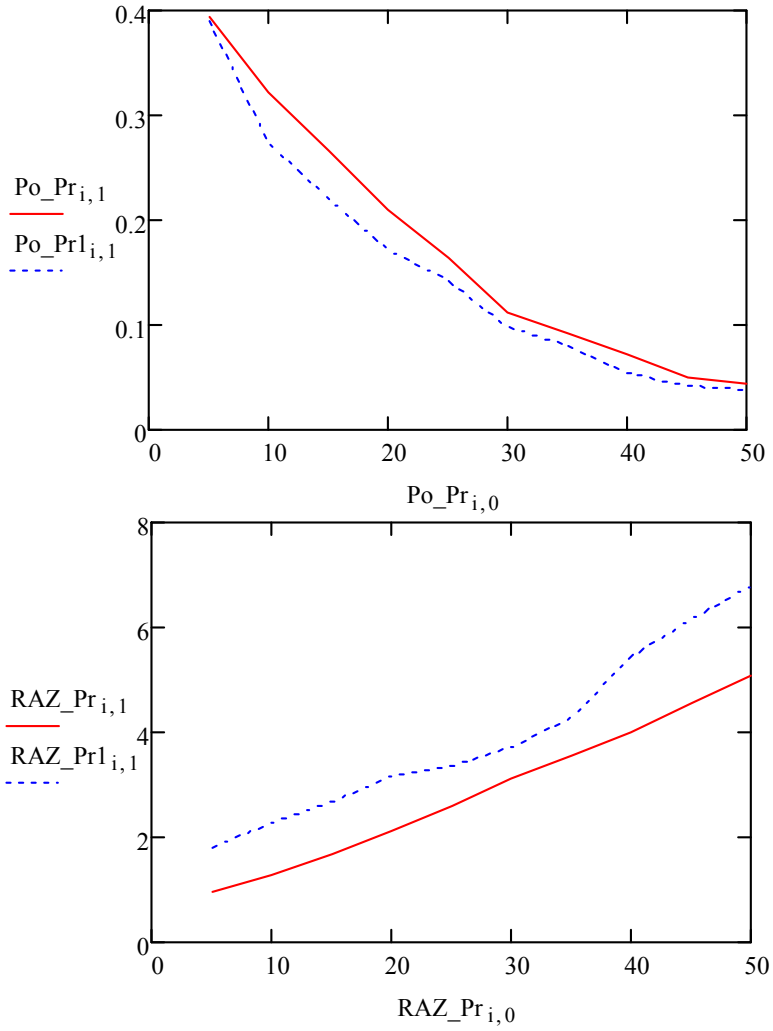


Рис. 5.24. Побудова емпіричних залежностей ймовірності помилкового вилучення інформаційних даних та середньої величини внесених спотворень до контейнер-зображення від величини порога «Pr»

Додаткове завдання. Реалізація алгоритмів вбудовування та вилучення повідомлень до частотної області зображень методом Дж. Фрідріх (пропонується до самостійного виконання

6. ПРИКЛАД ОФОРМЛЕННЯ ЗВІТУ З ЛАБОРАТОРНОЇ РОБОТИ

Лабораторна робота № 4
Метод Коха–Жао і його модифікації, метод Дж.Фрідріх

```
C :=READRGB("1.bmp")
R := READ_RED("1.bmp")
G := READ_GREEN( "1.bmp")
B := READ_BLUE("1.bmp")
M := READBIN("1.txt", "byte")
```

"1.bmp"

Функція перетворення числа із двійкового в десяткове:

$$D2B(x) := \left| \begin{array}{l} \text{for } i \in 0..7 \\ \quad V_i \leftarrow \text{mod}(x, 2) \\ \quad x \leftarrow \text{floor}\left(\frac{x}{2}\right) \\ V \end{array} \right.$$

Перетворимо повідомлення в двійковий вигляд:

$$m := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(M) - 1 \\ \quad b \leftarrow D2B\left(M_i\right) \\ \quad \text{for } j \in 0..7 \\ \quad\quad m_{8 \cdot i + j} \leftarrow b_j \\ m \end{array} \right.$$

$$N := 10 \qquad P := 1$$

$$C := \left| \begin{array}{l} \text{for } i \in 0..N - 1 \\ \quad C_i \leftarrow \frac{1}{\sqrt{2}} \text{ if } i = 0 \\ \quad C_i \leftarrow 1 \text{ if } i > 0 \\ C \end{array} \right.$$

$C =$

	0
0	0.707
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1

Функція прямого дискретно-косинусного перетворення Фур'є:

$$T(V) := \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \text{for } j \in 0..N-1 \\ \quad\quad T_{i,j} \leftarrow \text{round}\left[\frac{2}{N} \cdot C_i C_j \cdot \frac{1}{P} \cdot \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \left[V_{x,y} \cdot \cos\left[\frac{(2x+1)\cdot i \cdot \pi}{2N} \right] \cdot \cos\left[\frac{(2y+1)\cdot j \cdot \pi}{2N} \right] \right] \right] \\ T \end{array} \right.$$

Функція зворотного дискретно-косинусного перетворення Фур'є:

$$V(T) := \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \text{for } j \in 0..N-1 \\ \quad\quad V_{i,j} \leftarrow \text{round}\left[\sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \left[T_{x,y} \cdot P \cdot \frac{2}{N} \cdot C_x C_y \cdot \cos\left[\frac{(2i+1)\cdot x \cdot \pi}{2N} \right] \cdot \cos\left[\frac{(2j+1)\cdot y \cdot \pi}{2N} \right] \right] \right] \\ V \end{array} \right.$$

Розіб'ємо зображення на підблоки:

$$nn := \frac{\text{cols}(R)}{N} \qquad mm := \frac{\text{rows}(R)}{N}$$

$$r := \left| \begin{array}{l} \text{for } x \in 0..mm-1 \\ \quad \text{for } y \in 0..nn-1 \\ \quad\quad \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad \text{for } j \in 0..N-1 \\ \quad\quad RR_{i,j} \leftarrow R_{i+x\cdot N, j+y\cdot 8} \end{array} \right. \\ \quad\quad r_{x,y} \leftarrow RR \\ r \end{array} \right.$$

Здійснимо перетворення для кожного блоку:

$$tr := \left| \begin{array}{l} \text{for } i \in 0..mm-1 \\ \quad \text{for } j \in 0..nn-1 \\ \quad\quad tr_{i,j} \leftarrow T\left(r_{i,j}\right) \\ tr \end{array} \right.$$

Метод Коха–Жао

Вбудовування $Pr := 5$

$$(H1,H2) := \left| \begin{array}{l} -1 \\ 1 \text{ if } |H1| - |H2| > Pr \\ 0 \text{ if } |H1| - |H2| < -Pr \end{array} \right.$$

$$Input(TRR,m) := \left| \begin{array}{l} TRR \leftarrow TRR \\ \text{if } m = 1 \wedge m \neq H\left(TRR_{3,1}, TRR_{1,3}\right) \vee H\left(TRR_{3,1}, TRR_{1,3}\right) = -1 \\ \quad \left| \begin{array}{l} TRR_{3,1} \leftarrow |TRR_{1,3}| + Pr \text{ if } TRR_{3,1} > 0 \\ TRR_{3,1} \leftarrow -|TRR_{1,3}| - Pr \text{ if } TRR_{3,1} \leq 0 \end{array} \right. \\ \text{if } m = 0 \wedge m \neq H\left(TRR_{3,1}, TRR_{1,3}\right) \vee H\left(TRR_{3,1}, TRR_{1,3}\right) = -1 \\ \quad \left| \begin{array}{l} TRR_{1,3} \leftarrow |TRR_{3,1}| + Pr \text{ if } TRR_{1,3} > 0 \\ TRR_{1,3} \leftarrow -|TRR_{3,1}| - Pr \text{ if } TRR_{1,3} \leq 0 \end{array} \right. \\ Input \leftarrow TRR \end{array} \right.$$

```
tr := | num ← 0
      | for x ∈ 0.. mm − 1
      |   for y ∈ 0.. nn − 1
      |     | break if x·nn + y ≥ rows(m) − 1
      |     | tr_{x,y} ← Input(tr_{x,y}, m_num)
      |     | num ← num + 1
      | tr
```

```
vr := | for i ∈ 0.. mm − 1
      |   for j ∈ 0.. nn − 1
      |     vr_{i,j} ← V(tr_{i,j})
      | vr
```

Склеїмо блоки повідомлення:

```
R2 := | for x ∈ 0.. rows(vr) − 1
      |   for y ∈ 0.. cols(vr) − 1
      |     | temp1 ← vr_{x,y}
      |     | for i ∈ 0.. N − 1
      |     |   for j ∈ 0.. N − 1
      |     |     temp2_{x·N+i, y·N+j} ← temp1_{i,j}
      | temp2
```

```
R2 := | for i ∈ 0.. rows(R2) − 1
      |   for j ∈ 0.. cols(R2) − 1
      |     | R2_{i,j} ← 0 if R2_{i,j} < 0
      |     | R2_{i,j} ← 255 if R2_{i,j} > 255
      | R2
```

$vr_{1,0}$ =

	0	1	2	3	4
0	194	196	199	200	201
1	184	189	203	203	204
2	192	196	198	200	204
3	177	184	187	187	180
4	173	176	174	166	165
5	159	162	159	153	156
6	139	134	134	134	132
7	132	128	128	127	124
8	127	121	118	116	114
9	114	110	108	105	...

$r_{1,0}$ =

	0	1	2	3	4
0	195	196	199	200	201
1	185	189	202	203	203
2	192	196	198	199	204
3	177	185	187	186	180
4	173	176	174	166	165
5	160	162	158	153	156
6	139	134	134	134	132
7	132	128	128	127	125
8	126	121	118	117	115
9	113	110	108	106	...

Досліджуємо середнє значення спотворення внесеного зображення:

```
RAZ := | RAZ ← 0
       | for i ∈ 0.. rows(R2) − 1
       |   for j ∈ 0.. cols(R2) − 1
       |     RAZ ← RAZ + |R[i,j] − R2[i,j]|
       | RAZ ← RAZ / (rows(R)·cols(R))
       | RAZ
```

RAZ = 28.636

Вилучення:

```
tr1 := | for i ∈ 0.. mm − 1
       |   for j ∈ 0.. nn − 1
       |     tr[i,j] ← T(vr[i,j])
       | tr
```

```
m1 := | num ← 0
      | for x ∈ 0.. mm − 1
      |   for y ∈ 0.. nn − 1
      |     TRR1 ← tr1[x,y]
      |     m1[num] ← 1 if |TRR1[3,1]| > |TRR1[1,3]|
      |     m1[num] ← 0 if |TRR1[3,1]| ≤ |TRR1[1,3]|
      |     num ← num + 1
      | m1
```

m =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

m1 =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

Оцінимо імовірність помилки інформаційних біт:

```
Po := | Po ← 0
      | for i ∈ 0.. rows(m1) − 1
      |   Po ← Po + 1 if m[i] ≠ m1[i]
      | Po ← Po / rows(m1)
      | Po
```

Po = 0

```
G2 := | for i ∈ 0.. rows(R2) − 1
      |   for j ∈ 0.. cols(R2) − 1
      |     G2[i,j] ← G[i,j]
      | G2
```

```
B2 := | for i ∈ 0.. rows(R2) − 1
      |   for j ∈ 0.. cols(R2) − 1
      |     B2[i,j] ← B[i,j]
      | B2
```

Дослідження стійкості до атаки стисненням:

WRITERGB("Stego.bmp") := augment (R2, G2, B2)

"1"

"Stego"

R_Stego:=READ_RED ("Stego.jpg")

r2 :=
for $x \in 0..mm-1$
  for $y \in 0..nn-1$
    for $i \in 0..N-1$
      for $j \in 0..N-1$
        $RR_{i,j} \leftarrow R\_Stego_{i+x\cdot N, j+y\cdot N}$
    $r_{x,y} \leftarrow RR$
r

tr2 :=
for $i \in 0..mm-1$
  for $j \in 0..nn-1$
    $tr_{i,j} \leftarrow T(r2_{i,j})$
tr

m1 :=
num ← 0
for $x \in 0..mm-1$
  for $y \in 0..nn-1$
    $TRR1 \leftarrow tr2_{x,y}$
    $m1_{num} \leftarrow 1$ if $|TRR1_{3,1}| > |TRR1_{1,3}|$
    $m1_{num} \leftarrow 0$ if $|TRR1_{3,1}| \le |TRR1_{1,3}|$
    num ← num + 1
m1

m =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	...

m1 =

	0
0	1
1	1
2	1
3	0
4	1
5	0
6	1
7	0
8	1
9	0
10	1
11	1
12	1
13	1
14	0
15	...

Досліджуємо ймовірність помилки і побудуємо графіки:

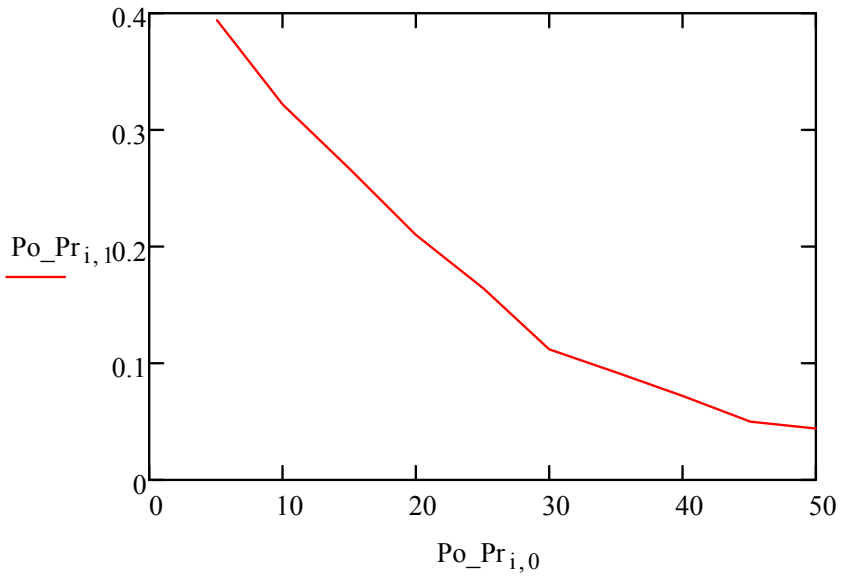
$$Po := \left| \begin{array}{l} Po \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(m1) - 1 \\ \quad Po \leftarrow Po + 1 \text{ if } m_i \neq m1_i \\ Po \leftarrow \dfrac{Po}{\text{rows}(m1)} \\ Po \end{array} \right.$$

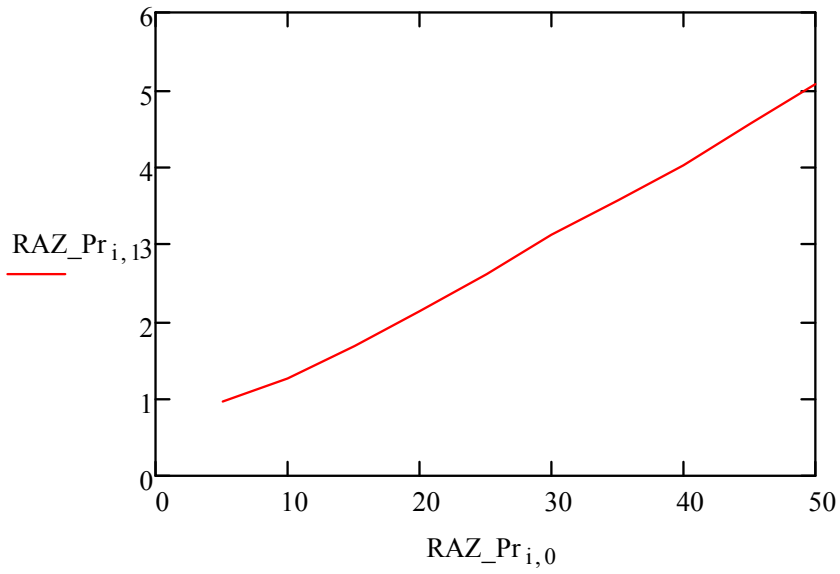
$Po = 0.522$

$i := 0..9$

$$Po\_Pr := \begin{pmatrix} 5 & 0.394 \\ 10 & 0.323 \\ 15 & 0.266 \\ 20 & 0.21 \\ 25 & 0.165 \\ 30 & 0.113 \\ 35 & 0.092 \\ 40 & 0.073 \\ 45 & 0.051 \\ 50 & 0.045 \end{pmatrix} \quad RAZ\_Pr := \begin{pmatrix} 5 & 0.974 \\ 10 & 1.273 \\ 15 & 1.692 \\ 20 & 2.134 \\ 25 & 2.601 \\ 30 & 3.121 \\ 35 & 3.568 \\ 40 & 4.012 \\ 45 & 4.560 \\ 50 & 5.069 \end{pmatrix}$$

$i := 0..9$





Модифікований метод:

Здійснимо перетворення Фур'є для кожного блоку:

$$tr := \left| \begin{array}{l} \text{for } i \in 0..mm-1 \\ \quad \text{for } j \in 0..nn-1 \\ \quad\quad tr_{i,j} \leftarrow T\left(r_{i,j}\right) \\ tr \end{array} \right.$$

$$Input(TRR, m) := \left| \begin{array}{l} \text{if } m = 1 \\ \quad \left| \begin{array}{l} TRR_{3,1} \leftarrow \left|TRR_{1,3}\right| + Pr \text{ if } TRR_{3,1} > 0 \\ TRR_{3,1} \leftarrow -\left|TRR_{1,3}\right| - Pr \text{ if } TRR_{3,1} \le 0 \\ TRR_{3,2} \leftarrow \left|TRR_{1,3}\right| + Pr \text{ if } TRR_{3,2} > 0 \\ TRR_{3,2} \leftarrow -\left|TRR_{1,3}\right| - Pr \text{ if } TRR_{3,2} \le 0 \end{array} \right. \\ \text{if } m = 0 \\ \quad \left| \begin{array}{l} TRR_{1,3} \leftarrow \left|TRR_{3,1}\right| + Pr \text{ if } TRR_{1,3} > 0 \\ TRR_{1,3} \leftarrow -\left|TRR_{3,1}\right| - Pr \text{ if } TRR_{1,3} \le 0 \\ TRR_{2,3} \leftarrow \left|TRR_{3,1}\right| + Pr \text{ if } TRR_{2,3} > 0 \\ TRR_{2,3} \leftarrow -\left|TRR_{3,1}\right| - Pr \text{ if } TRR_{2,3} \le 0 \end{array} \right. \\ TRR \end{array} \right.$$

$$tr := \left| \begin{array}{l} num \leftarrow 0 \\ \text{for } x \in 0..mm-1 \\ \quad \text{for } y \in 0..nn-1 \\ \quad\quad \left| \begin{array}{l} \text{break if } x \cdot nn + y \ge \text{rows}(m) - 1 \\ tr_{x,y} \leftarrow Input\left(tr_{x,y}, m_{num}\right) \\ num \leftarrow num + 1 \end{array} \right. \\ tr \end{array} \right.$$

$$vr := \left| \begin{array}{l} \text{for } i \in 0..mm-1 \\ \quad \text{for } j \in 0..nn-1 \\ \quad\quad vr_{i,j} \leftarrow V\left(tr_{i,j}\right) \\ vr \end{array} \right.$$

Склеїмо блоки повідомлення:

$$
\begin{aligned}
R2 := \;& \text{for } x \in 0..\text{rows}(vr) - 1 \\
& \quad \text{for } y \in 0..\text{cols}(vr) - 1 \\
& \quad\quad temp1 \leftarrow vr_{x,y} \\
& \quad\quad \text{for } i \in 0..N - 1 \\
& \quad\quad\quad \text{for } j \in 0..N - 1 \\
& \quad\quad\quad\quad temp2_{x\cdot N+i,\, y\cdot N+j} \leftarrow temp1_{i,j} \\
& temp2
\end{aligned}
$$

$$
\begin{aligned}
R2 := \;& \text{for } i \in 0..\text{rows}(R2) - 1 \\
& \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\
& \quad\quad R2_{i,j} \leftarrow 0 \text{ if } R2_{i,j} < 0 \\
& \quad\quad R2_{i,j} \leftarrow 255 \text{ if } R2_{i,j} > 255 \\
& R2
\end{aligned}
$$

Дослідимо середнє значення спотворення, внесеного в зображення:

$$
\begin{aligned}
RAZ := \;& RAZ \leftarrow 0 \\
& \text{for } i \in 0..\text{rows}(R2) - 1 \\
& \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\
& \quad\quad RAZ \leftarrow RAZ + \left| R_{i,j} - R2_{i,j} \right| \\
& RAZ \leftarrow \frac{RAZ}{\text{rows}(R)\cdot\text{cols}(R)} \\
& RAZ
\end{aligned}
$$

$RAZ = 28.649$

Вилучення :

$$
\begin{aligned}
tr1 := \;& \text{for } i \in 0..mm - 1 \\
& \quad \text{for } j \in 0..nn - 1 \\
& \quad\quad tr_{i,j} \leftarrow T\left(vr_{i,j}\right) \\
& tr
\end{aligned}
$$

R

R2

Досліджуємо середнє значення спотворення, внесеного в зображення:

$$RAZ := \left| \begin{array}{l} RAZ \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(R2) - 1 \\ \quad \text{for } j \in 0..\text{cols}(R2) - 1 \\ \quad\quad RAZ \leftarrow RAZ + \left| R_{i,j} - R2_{i,j} \right| \\ RAZ \leftarrow \dfrac{RAZ}{\text{rows}(R)\cdot\text{cols}(R)} \\ RAZ \end{array} \right.$$

$RAZ = 28.649$

Вилучення :

$$tr1 := \left| \begin{array}{l} \text{for } i \in 0..mm - 1 \\ \quad \text{for } j \in 0..nn - 1 \\ \quad\quad tr_{i,j} \leftarrow T\left(vr_{i,j}\right) \\ tr \end{array} \right.$$

$$m1 := \left| \begin{array}{l} num \leftarrow 0 \\ \text{for } x \in 0..mm - 1 \\ \quad \text{for } y \in 0..nn - 1 \\ \quad\quad TRR1 \leftarrow tr1_{x,y} \\ \quad\quad m1_{num} \leftarrow 1 \text{ if } \left|TRR1_{3,1}\right| > \left|TRR1_{1,3}\right| \wedge \left|TRR1_{3,2}\right| > \left|TRR1_{1,3}\right| \\ \quad\quad m1_{num} \leftarrow 0 \text{ if } \left|TRR1_{3,1}\right| \le \left|TRR1_{1,3}\right| \wedge \left|TRR1_{3,2}\right| \le \left|TRR1_{1,3}\right| \\ \quad\quad num \leftarrow num + 1 \\ m1 \end{array} \right.$$

$$Po := \left| \begin{array}{l} Po \leftarrow 0 \\ \text{for } i \in 0..\text{rows}(m1) - 1 \\ \quad Po \leftarrow Po + 1 \text{ if } m_i \neq m1_i \\ Po \leftarrow \dfrac{Po}{\text{rows}(m1)} \\ Po \end{array} \right.$$

$Po = 0$

m =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	…

m1 =

	0
0	0
1	0
2	0
3	1
4	0
5	0
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	1
14	1
15	…

Дослідження стійкості до атаки стисненням:

WRITERGB ("Stego2.bmp") := augment (R2, G2, B2)

"1"

"Stego2"

$R\_Stego := READ\_RED("Stego2.jpg")$

```
r2 := | for x ∈ 0.. mm − 1
      |   for y ∈ 0.. nn − 1
      |     for i ∈ 0.. N − 1
      |       for j ∈ 0.. N − 1
      |         RR[i,j] ← R_Stego[i+x·N, j+y·N]
      |     r[x,y] ← RR
      | r
```

```
tr2 := | for i ∈ 0.. mm − 1
       |   for j ∈ 0.. nn − 1
       |     tr[i,j] ← T(r2[i,j])
       | tr
```

```
m1 := | num ← 0
      | for x ∈ 0.. mm − 1
      |   for y ∈ 0.. nn − 1
      |     TRR1 ← tr2[x,y]
      |     m1[num] ← 1 if |TRR1[3,1]| > |TRR1[1,3]| ∧ |TRR1[3,2]| > |TRR1[1,3]|
      |     m1[num] ← 0 if |TRR1[3,1]| ≤ |TRR1[1,3]| ∧ |TRR1[3,2]| ≤ |TRR1[1,3]|
      |     num ← num + 1
      | m1
```

Дослідимо імовірність помилки і побудуємо графіки:

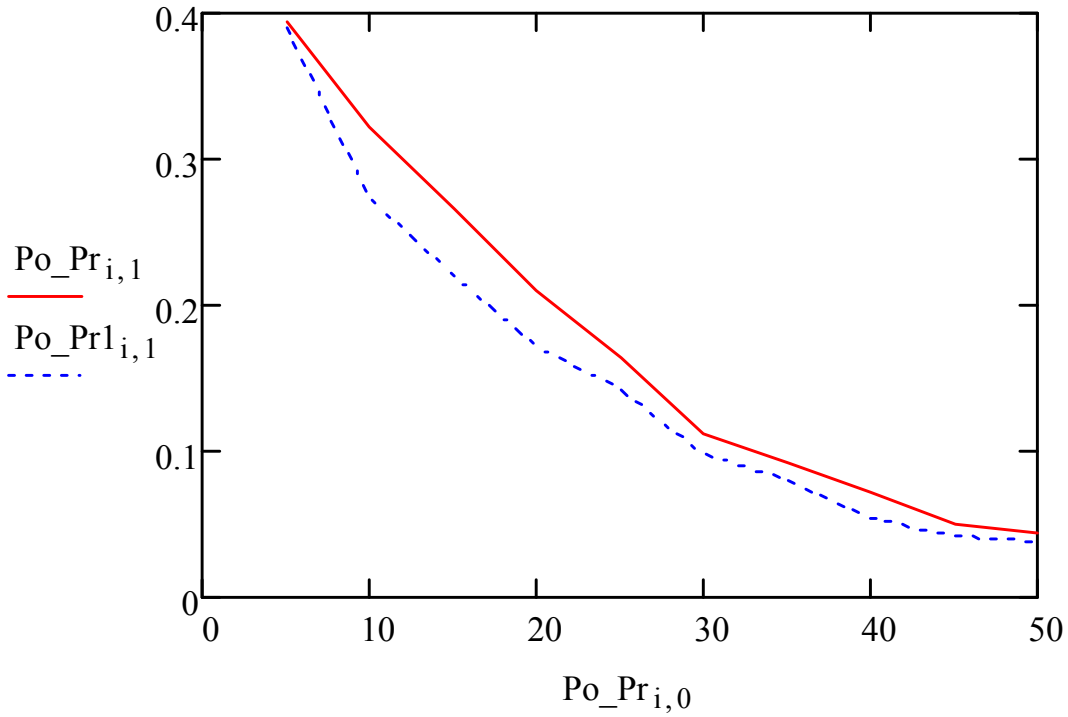
```
Po := | Po ← 0
      | for i ∈ 0.. rows(m1) − 1
      |   Po ← Po + 1 if m_i ≠ m1_i
      | Po ← Po / rows(m1)
      | Po
```

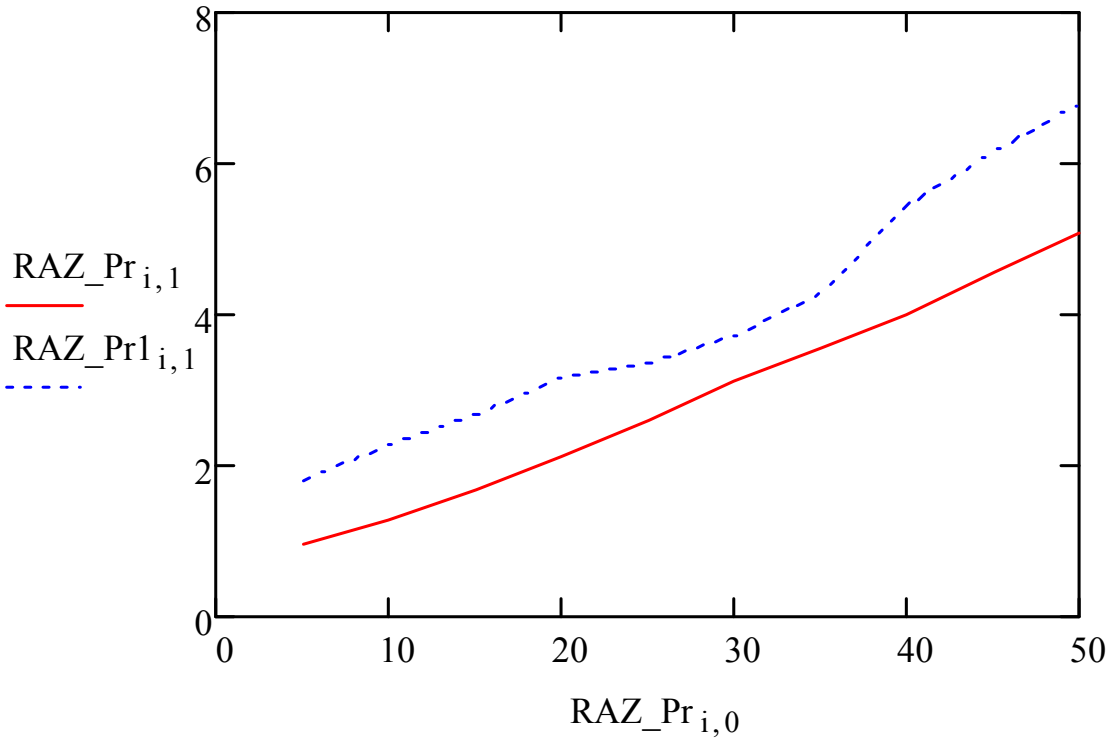
$Po = 0.542$

$i := 0..9$

$$Po\_Pr1 := \begin{pmatrix} 5 & 0.391 \\ 10 & 0.275 \\ 15 & 0.221 \\ 20 & 0.173 \\ 25 & 0.142 \\ 30 & 0.099 \\ 35 & 0.081 \\ 40 & 0.055 \\ 45 & 0.042 \\ 50 & 0.038 \end{pmatrix} \quad RAZ\_Pr1 := \begin{pmatrix} 5 & 1.815 \\ 10 & 2.273 \\ 15 & 2.692 \\ 20 & 3.142 \\ 25 & 3.351 \\ 30 & 3.721 \\ 35 & 4.298 \\ 40 & 5.431 \\ 45 & 6.169 \\ 50 & 6.801 \end{pmatrix} \quad Po\_Pr := \begin{pmatrix} 5 & 0.394 \\ 10 & 0.323 \\ 15 & 0.266 \\ 20 & 0.21 \\ 25 & 0.165 \\ 30 & 0.113 \\ 35 & 0.092 \\ 40 & 0.073 \\ 45 & 0.051 \\ 50 & 0.045 \end{pmatrix} \quad RAZ\_Pr := \begin{pmatrix} 5 & 0.974 \\ 10 & 1.273 \\ 15 & 1.692 \\ 20 & 2.134 \\ 25 & 2.601 \\ 30 & 3.121 \\ 35 & 3.568 \\ 40 & 4.012 \\ 45 & 4.560 \\ 50 & 5.069 \end{pmatrix}$$

$i := 0..9$


0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
Po_Pr i, 1
Po_Pr1 i, 1
Po_Pr i, 0


8
6
4
2
0
0
10
20
30
40
50
RAZ_Pr i, 1
RAZ_Pr1 i, 1
RAZ_Pr i, 0

Навчальне видання

Кузнецов Олександр Олександрович
Полуяненко Микола Олександрович
Кузнецова Тетяна Юріївна

ПРИХОВУВАННЯ ДАНИХ У ЧАСТОТНІЙ ОБЛАСТІ НЕРУХОМИХ ЗОБРАЖЕНЬ НА ОСНОВІ КОДУВАННЯ РІЗНИЦІ АБСОЛЮТНИХ ЗНАЧЕНЬ КОЕФІЦІЄНТІВ ДИСКРЕТНО-КОСИНУСНОГО ПЕРЕТВОРЕННЯ

Методичні рекомендації
до лабораторної роботи з дисципліни «Стеганографія»
для студентів спеціальності 125 «Кібербезпека»

Коректор *А. І. Самсонова*
Комп'ютерне верстання *Л. П. Зябченко*
Макет обкладинки *І. М. Дончик*

Формат 60×84/16. Ум. друк. арк. 2,9. Наклад 50 пр. Зам. № 141/19.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009

Видавництво ХНУ імені В. Н. Каразіна
Тел. 705-24-32