Міністерство освіти та науки України
Одеський національний морський університет

КОБОЗЄВА АЛЛА АНАТОЛІЇВНА

ОСНОВИ СТЕГАНОГРАФІЇ

Конспект лекцій

для здобувачів
першого (бакалаврського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації

Одеса-2025

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

Конспект лекцій схвалено на засіданні кафедри «Кібербезпека та захист інформації»
(Протокол від «06» жовтня 2025 р. №2)

Конспект лекцій схвалено на засіданні НМК ННІ ІТІП
(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

Тема 1. Цифрове зображення та його обробка 3
Тема 2. Перетворення Фурьє 14
Тема 3. Стиск цифрових зображень 23
Тема 4. Основні поняття цифрової стеганографії 33
Тема 5. Організація прихованого каналу зв’язку 38
Тема 6. Властивості стеганосистеми 42
Тема 7. Стеганоперетворення в частотній області контейнера. Метод Коха і Жао 50
Тема 8. Стеганографічний метод, що забезпечує високу пропускну спроможність прихованого каналу зв'язку 54
Тема 9. Стеганоперетворення, стійке до атаки стиском 59
Література 66

Тема 1. ЦИФРОВЕ ЗОБРАЖЕННЯ ТА ЙОГО ОБРОБКА

План

1. Цифрове зображення.
2. Просторові методи поліпшення зображення. Деякі градаційні перетворення. Гістограма зображення. Основи просторової фільтрації.

1. Цифрове зображення

Зображення можна визначити як функцію $f(x,y)$, де x,y - координати на площині, значення f якої в будь-якій точці, що задається парою координат $(x,y) \in D \subseteq R^2$, називається ***інтенсивністю*** або ***рівнем сірого***, або ***градацією сірого***, або ***яскравістю*** в цій точці. Якщо величини x,y,f приймають скінченне число дискретних значень, то говорять про ***цифрове зображення*** (ЦЗ). Цифровою обробкою зображень називається обробка ЦЗ за допомогою комп'ютера. ЦЗ складається зі скінченного числа елементів, кожний з яких розташований у конкретному місці й приймає певне значення. Ці елементи називаються елементами зображення або ***пікселями***.

Щоб одержати ЦЗ, необхідно перетворити неперервний сигнал у цифрову форму. Ця операція містить у собі 2 процеси: ***дискретизацію*** й ***квантування***.

Головний принцип, що лежить в основі дискретизації й квантування, проілюстрований на рис.1.1 (рисунки, що використані в темі 1, взяти з джерела: *Gonzalez R., Woods R. Digital Image Processing (4th Ed.). Pearson, 2018. 1020 p.*). Тут наведене вхідне зображення $f(x,y)$, яке ми хочемо перетворити в цифрову форму. Зображення неперервне по координатах x,y, а також по амплітуді f. Щоб перетворити цю функцію в цифрову форму, необхідно представити її відліками по обом координатам і по амплітуді. Представлення координат у вигляді скінченної множини відліків називається ***дискретизацією***, а представлення амплітуди значеннями зі скінченної множини - ***квантуванням***.

У результаті операцій дискретизації й квантування в загальному випадку виникає матриця дійсних чисел.

Припустимо, що в результаті дискретизації зображення $f(x,y)$ отримана матриця з M рядків і N стовпців. Координати (x,y) стають тепер дискретними значеннями. Для зручності будемо використовувати для цих координат цілі значення (рис.1.2).

Треба пам'ятати, що позначення, наприклад, (0,1) використовується лише для вказівки на другий відлік у першому рядку, і не означає, що це фактичні значення фізичних координат точок дискретизації.

Тоді повне ЦЗ ми можемо компактно записати у вигляді матриці:

$$f(x,y) = \begin{pmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \dots & \dots & \dots & \dots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{pmatrix}.$$

Кожний елемент цієї матриці - елемент зображення, або піксель. Далі будемо використовувати більш традиційний матричний запис:

$$A = \begin{pmatrix} a_{00} & a_{01} & \dots & a_{0,N-1} \\ a_{10} & a_{11} & \dots & a_{1,N-1} \\ \dots & \dots & \dots & \dots \\ a_{M-1,0} & a_{M-1,1} & \dots & a_{M-1,N-1} \end{pmatrix}$$

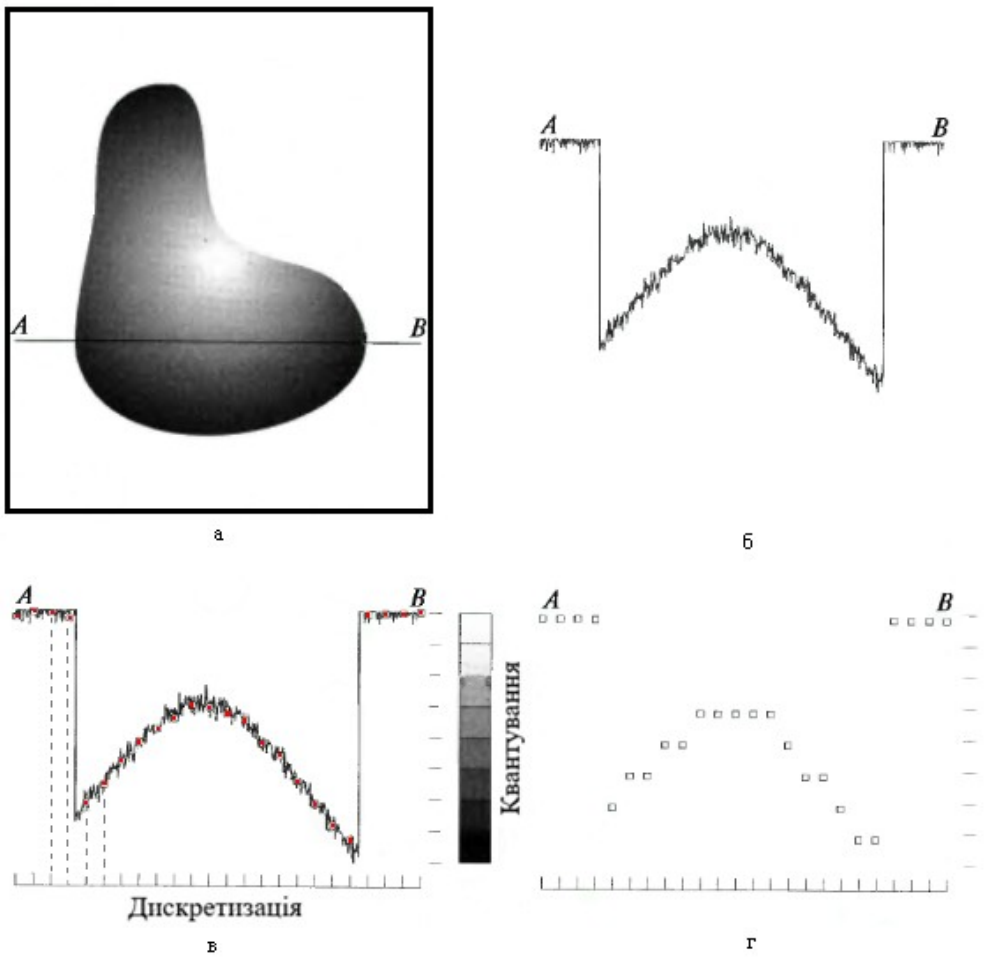


Рис.1.1. Формування ЦЗ. Неперервне зображення (а). Профіль уздовж лінії сканування між точками А і В на неперервному зображенні, який використовується для ілюстрації понять дискретизація й квантування (б). Дискретизація і квантування (в). Цифрове представлення рядка зображення (г)

Для виконання процесу оцифровки зображення необхідно прийняти угоду щодо значень M и N, а також числа рівнів (градацій) яскравості L, дозволених для кожного пікселя. Для M і N не існує спеціальних вимог крім того, що вони повинні бути натуральними. А значення L, з міркувань зручності побудови встаткування для обробки, зберігання й дискретизації, зазвичай вибирають $L = 2^k, k \in N$, де N - множина натуральних чисел. Ми припускаємо, що дискретні рівні яскравості розташовані з постійним кроком (тобто використовується рівномірне квантування) і приймають цілі значення в інтервалі $[0, L-1]$. Інтервал значень яскравості називають ***динамічним діапазоном зображення***.

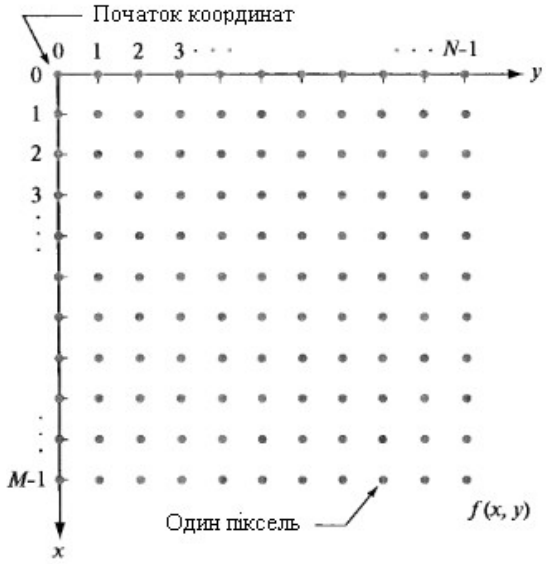


Рис.1.2. Система координат для представлення цифрових зображень

Дискретизація є головним чинником, що визначає ***просторову роздільну здатність*** зображення. По суті, просторова роздільна здатність - це розмір найменших помітних деталей на зображенні.

Яскравосною або ***півтоновою роздільною здатністю*** називається найменша помітна зміна яскравості. При виборі числа градацій яскравості доводиться в значній мірі враховувати особливості апаратури. Найбільш частим є вибір 8-бітного представлення (256 градацій сірого).

У якості дуже грубого емпіричного правила можна вважати, що мінімальні просторова і півтонова роздільна здатність, при яких ЦЗ буде відносно вільним від дефектів типу неправильних контурів і ступінчастості, становить близько 256*256 пікселів з 64 градаціями яскравості.

2. Просторові методи поліпшення зображення. Деякі градаційні перетворення. Гістограма зображення. Основи просторової фільтрації.

Головна мета поліпшення ЦЗ полягає в такій його обробці, щоб результат виявився більш підходящим з погляду конкретного застосування.

Множина підходів до поліпшення ЦЗ розпадається на дві великі категорії: методи обробки в просторовій області й методи обробки в частотній області. Термін просторова область відноситься до площини зображення (маніпуляції безпосередньо з пікселями зображення). Методи в частотній області ґрунтуються на модифікації сигналу, формованого шляхом застосування до ЦЗ перетворення Фур'є.

Загальної теорії поліпшення зображень не існує.

Просторова область - це множина пікселів, що складають ЦЗ.

Процедури просторової обробки описуються загальним рівнянням:

$$g(x,y) = T\left[f(x,y)\right]$$

де $f(x,y)$ - вхідне ЦЗ, $g(x,y)$ - оброблене, а T – оператор над f, що визначений в деякому околі точки (x,y), для якої ця точка є центром (рис.1.3). Центр околу пересувається від пікселя до пікселя, починаючи з верхнього лівого кута. Оператор T виконується для кожної точки (x,y), даючи в результаті вихідне значення g для даної точки. Процес використовує тільки пікселі усередині області ЦЗ, обмеженої околом (рис.1.3).

Рис.1.3. Окіл 3*3 для точки (x, y) ЦЗ

Найпростіша форма оператора T досягається, коли окіл має розміри 1*1 (один піксель). В цьому випадку g залежить тільки від значення f в точці (x, y), і T називається ***функцією градаційного перетворення*** (***функцією перетворення інтенсивностей*** або ***функцією відображення***) виду

$$s = T(r),$$

де r, s - змінні, що позначають відповідно значення яскравостей зображень $f(x, y)$ і $g(x, y)$ в кожній точці (x, y). Наприклад, якщо $T(r)$ має вид, показаний на рис.1.4, то ефектом від такого перетворення буде посилення контрасту. В граничному випадку (рис.1.4(б)) $T(r)$ дає бінарне ЦЗ. Відображення такої форми називається ***пороговою функцією***.

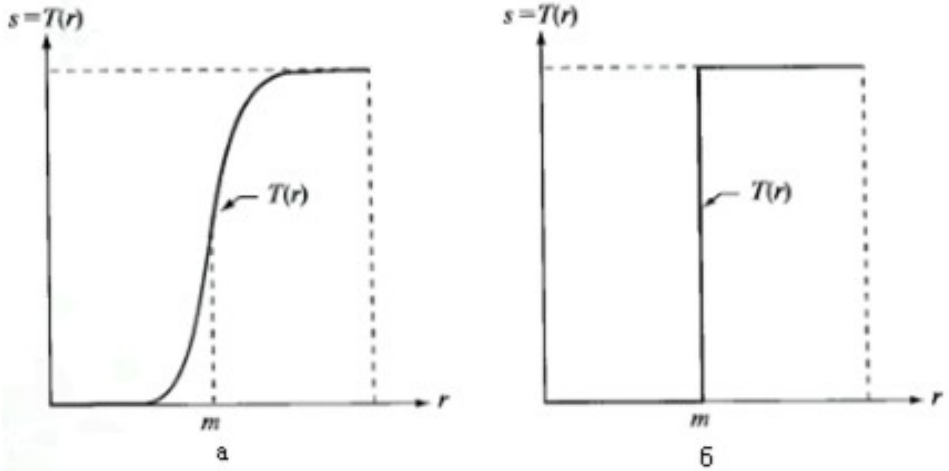


Рис.1.4. Градаційне перетворення для поліпшення контрасту

Деякі основні градаційні перетворення

Рис.1.5 – три основних типи перетворень:

- Лінійне (негатив: перетворення ЦЗ з яскравостями в діапазоні $[0, L-1]$ визначається виразом $s = L-1-r$ (рис.1.6); тотожне перетворення: $s = r$);
- Логарифмічне (загальний вид: $s = c\log(1+r)$, $c = const, r \geq 0$);
- Степеневе (загальний вид: $s = cr^{\gamma}$, $c, \gamma = const$, $c, \gamma > 0$).

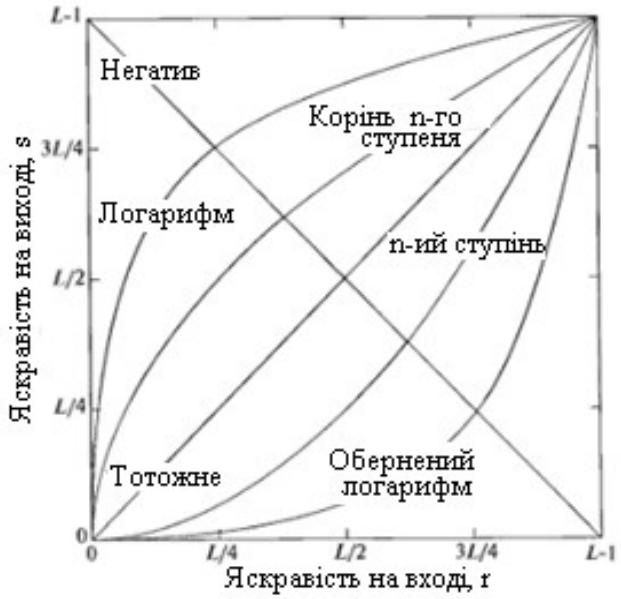


Рис. 1.5. Деякі основні функції градаційних перетворень, які використовуються для поліпшення зображень

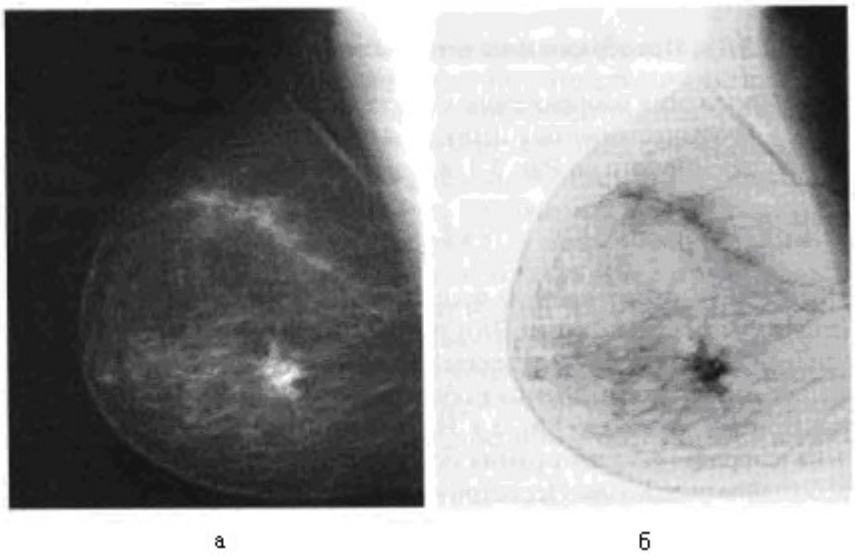


Рис.1.6. а - Вхідний вигляд рентгенограми молочної залози; б - негативне зображення, отримане застосуванням негативного перетворення

Приклад. *Поліпшення контрастів за допомогою степеневих перетворень* (рис.1.7). Зображення переважно темне, бажане здійснити розтягання рівнів яскравості. Це може бути досягнуте за допомогою степеневого перетворення з показником ступеня менше 1.

Приклад. Потрібно поліпшити зображення, яке виглядає таким, «що вилиняло» (рис.1.8). Це досягається шляхом степеневих перетворень із показником ступеня більше 1.

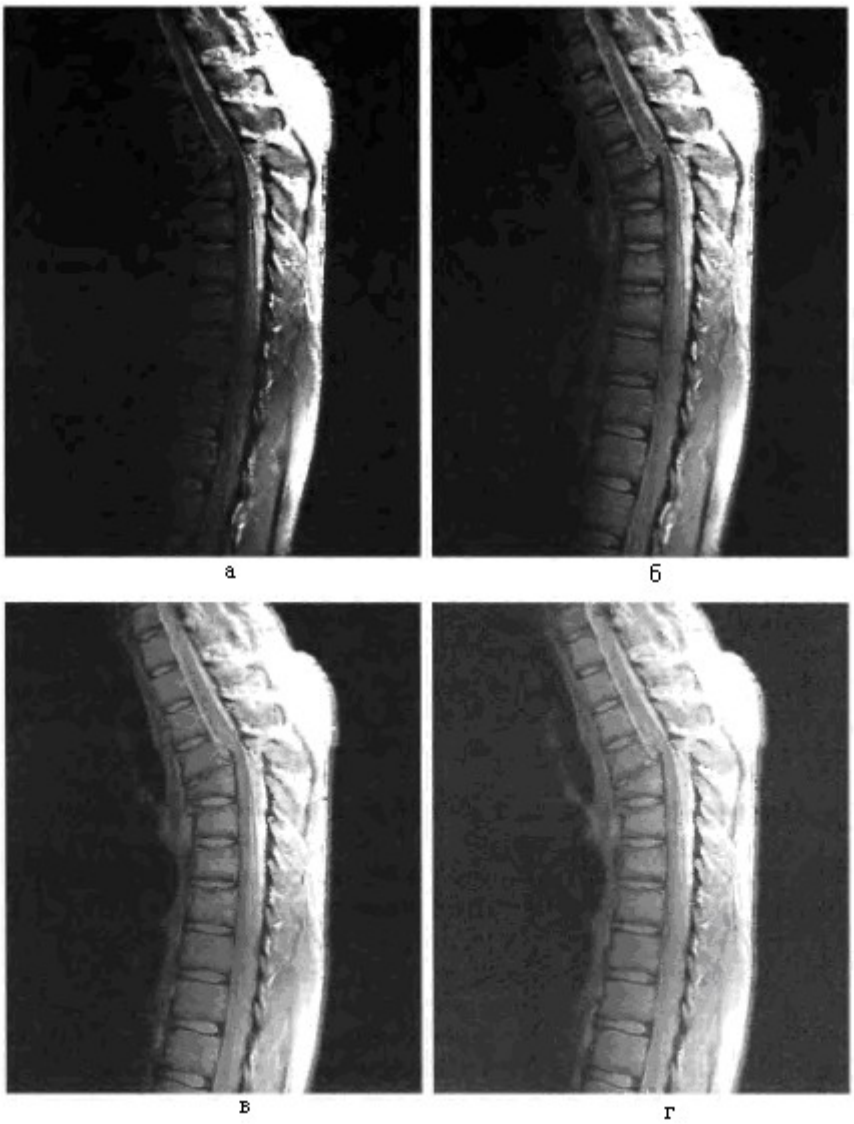


Рис.1.7. а - Знімок хребта людини з переломом (ЦЗ отримане за допомогою ЯМР-томографа); б-г - результати перетворень з c=1 і $\gamma = 0.6, 0.4, 0.3$ відповідно

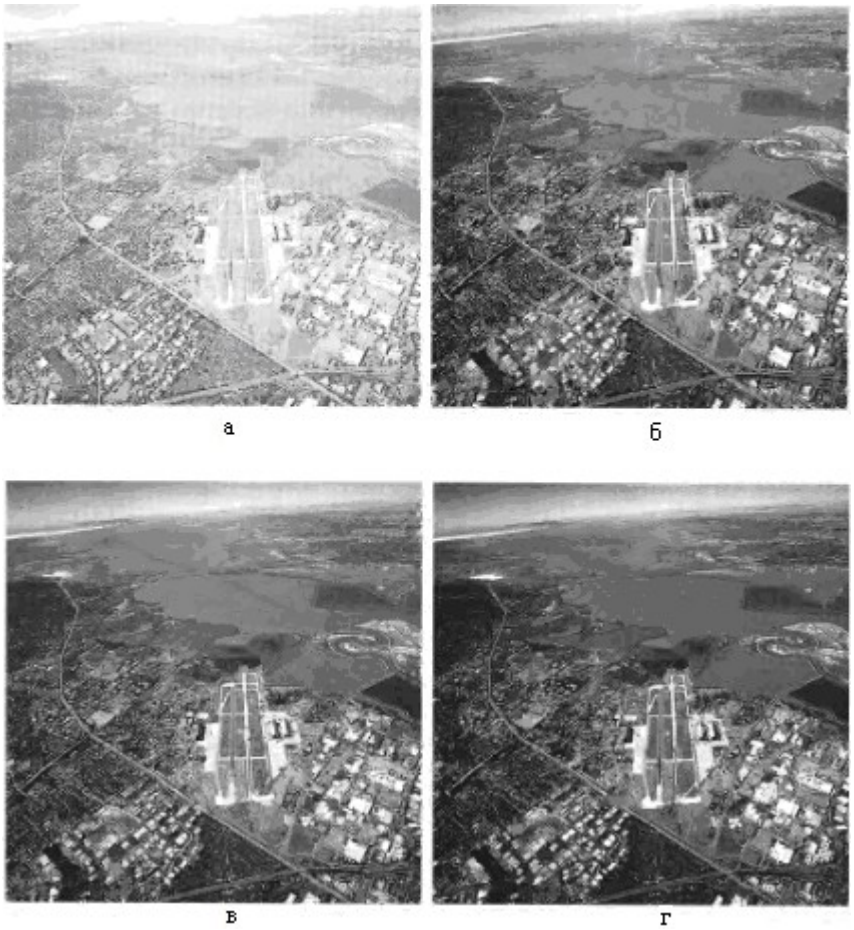


Рис.1.8. а – Аерофотознімок; б-г - результати перетворення з c=1 і $\gamma = 3.0, 4.0, 5.0$ відповідно

Дуже важливим об'єктом, використовуваним у процесі обробки ЦЗ, є його гістограма. ***Гістограмою*** ЦЗ з рівнями яскравості в діапазоні $[0, L-1]$ називається дискретна функція $h(r_k) = n_k$, де r_k - це $k-$й рівень яскравості, а n_k - число пікселів на ЦЗ, що мають яскравість r_k. Загальною практикою є нормалізація гістограми шляхом ділення кожного з її значень на загальне число пікселів у ЦЗ, яке позначається n. Тоді значення нормалізованої гістограми будуть $p(r_k) = n_k / n$. Сума всіх значень нормалізованої гістограми дорівнює 1. Видозміна гістограми може успішно використовуватися для поліпшення ЦЗ.

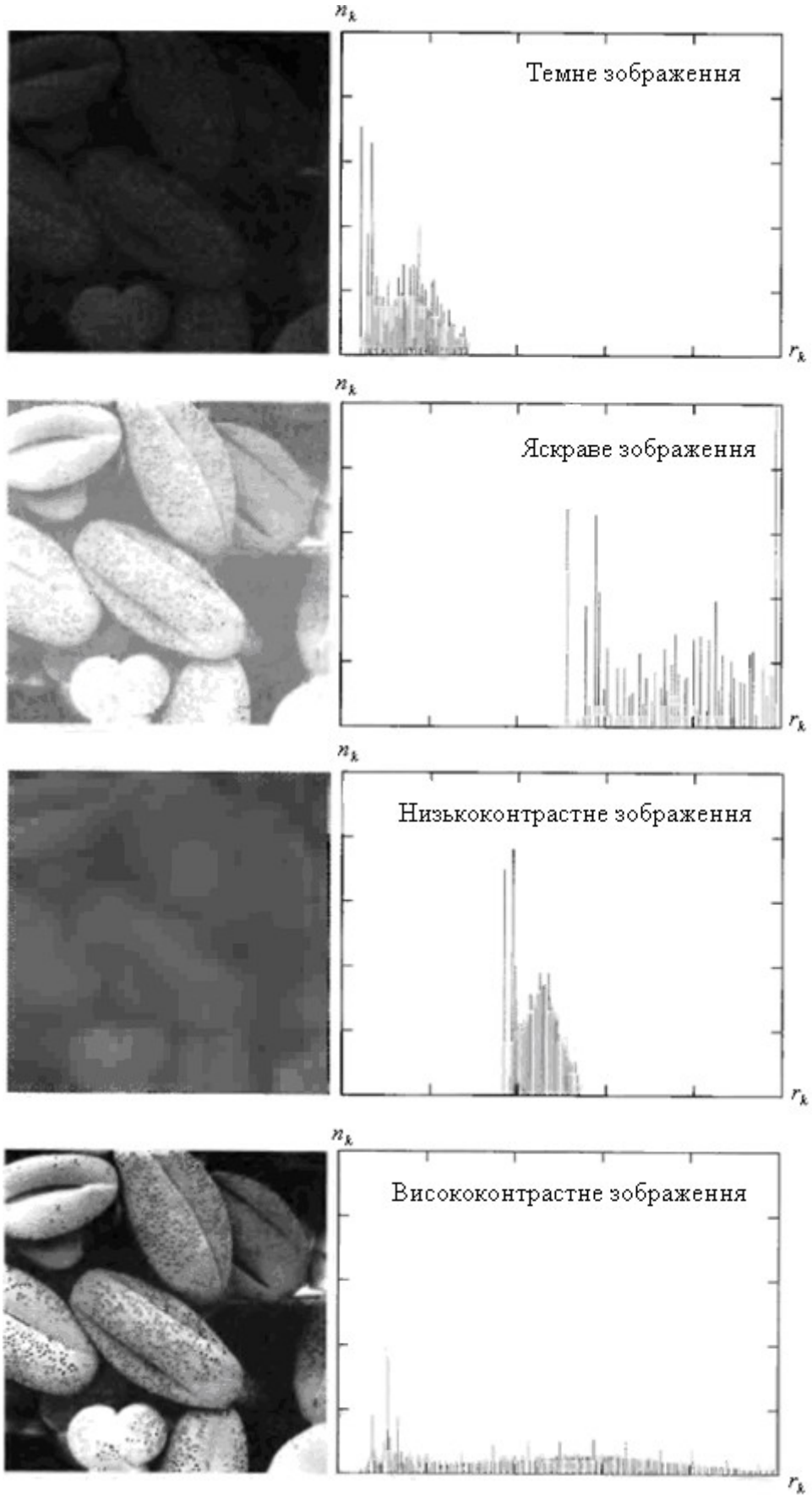


Рис.1.9. Чотири основні типи зображень

Один із часто використовуваних способів обробки зображення, яка виконується з різними цілями, є просторова фільтрація. *Просторова фільтрація* - фільтрація, яка виконується безпосередньо над елементами ЦЗ. Схема просторової фільтрації представлена на рис.1.10. Процес заснований на простому переміщенні маски фільтра від точки до точки ЦЗ; у кожній точці відгук фільтра обчислюється з використанням попередньо заданих зв'язків.

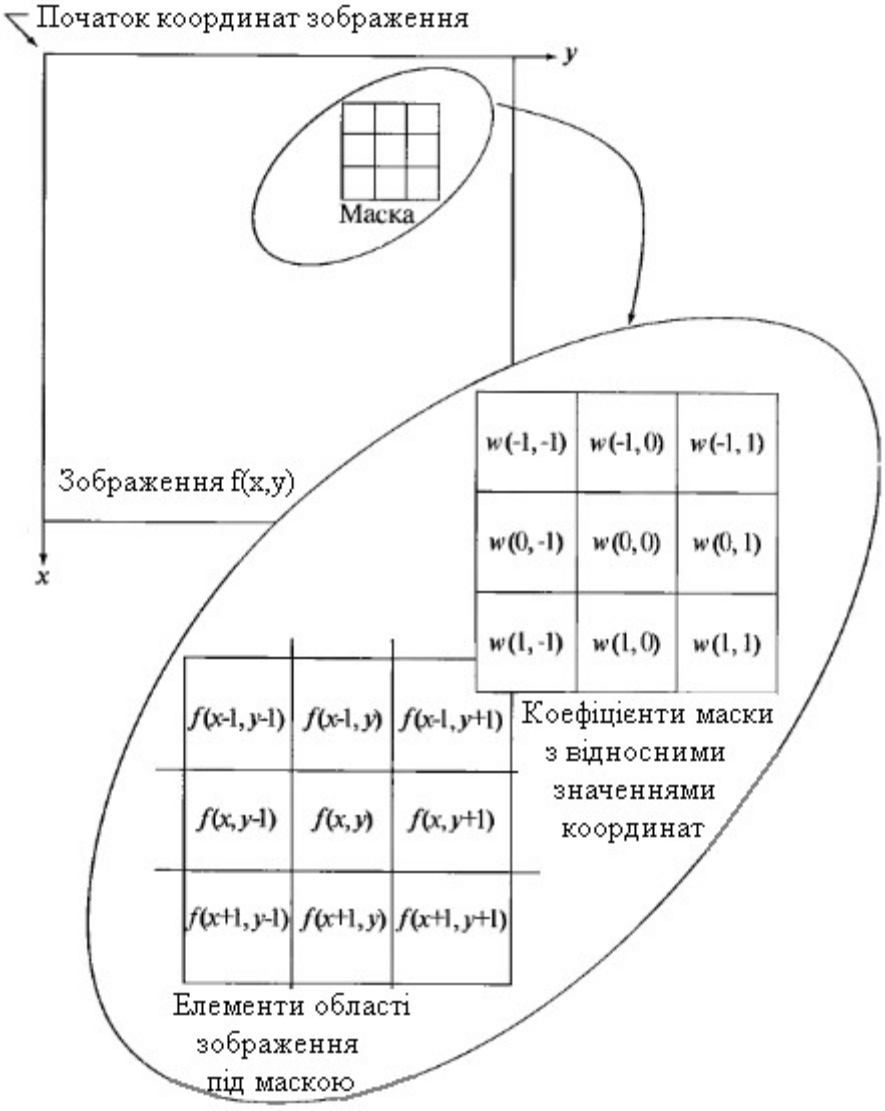


Рис.1.10. Схема просторової фільтрації

У випадку лінійної просторової фільтрації відгук задається сумою добутків коефіцієнтів фільтра на відповідні значення пікселів в області, покритої маскою. Для маски 3*3 (рис.1.10), результат (відгук) R лінійної фільтрації в точці (x, y) обчислюється як

$$R = w(-1,-1)f(x-1,y-1) + w(-1,0)f(x-1,y) + ... + w(0,0)f(x,y) + ... + w(1,0)f(x+1,y) +$$

$$+ w(1,1)f(x+1,y+1)$$

Відгук найпростішого лінійного просторового фільтра, що згладжує, є середнє значення елементів по околу, покритому маскою фільтра (рис.1.11). Такі фільтри називають ***усереднюючими*** або ***фільтрами, що згладжують***. Далі вони також будуть

називатися ***низькочастотними*** фільтрами. Ідея: заміною вхідних значень елементів ЦЗ на середні значення по масці фільтра досягається зменшення «різких» переходів рівнів яскравості, придушення шумів. Однак контури також характеризуються різкими перепадами яскравості, тому негативною стороною застосування фільтрів, що згладжують, є розфокусировка контурів, однак такі фільтри дозволяють згладжувати неправильні контури, які виникають при перетвореннях з недостатнім числом рівнів яскравості.

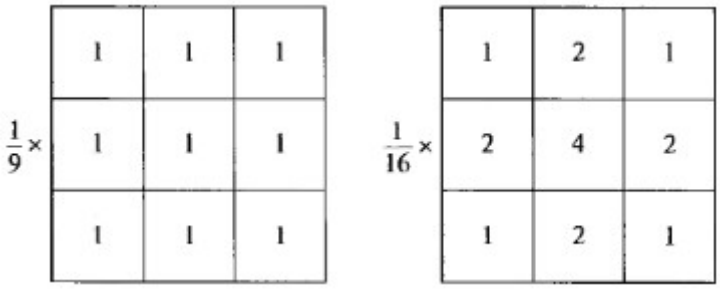


Рис.1.11. Дві маски фільтрів, що згладжують, по околу 3*3

Фільтр, маска якого представлена на рис.1.11(а) – всі коефіцієнти однакові – називається ***однорідним усереднюючим фільтром***. Маска на рис.1.11(б) дає так зване ***зважене середнє***: коефіцієнт у центрі маски має найбільше значення (вагу), тим самим даючи відповідному елементу більшу важливість при обчисленні середнього. Значення інших коефіцієнтів у масці зменшується з видаленням від центру маски. Основна стратегія присвоєння центральному пікселю найбільшої ваги, а іншим - оберненопропорційно їх відстані до центру, має на меті зменшення розфокусировки при згладжуванні.

Застосування просторового згладжування, що приводить до розфокусировки зображення, дозволяє створити грубий образ об'єктів, які можуть становити інтерес. При цьому інтенсивність дрібних об'єктів змішується із тлом, у той час як великі об'єкти залишаються у вигляді плям і можуть бути легко виявлені. Розміри об'єктів, які будуть змішуватися із тлом, приблизно збігаються з розмірами маски фільтра, що згладжує. Приклад на рис.1.12. Результат на рис.1.12(в) є більш прийнятним, чим вхідне зображення, для задачі пошуку самих великих і яскравих об'єктів.

Існують і інші принципи побудови масок фільтрів.

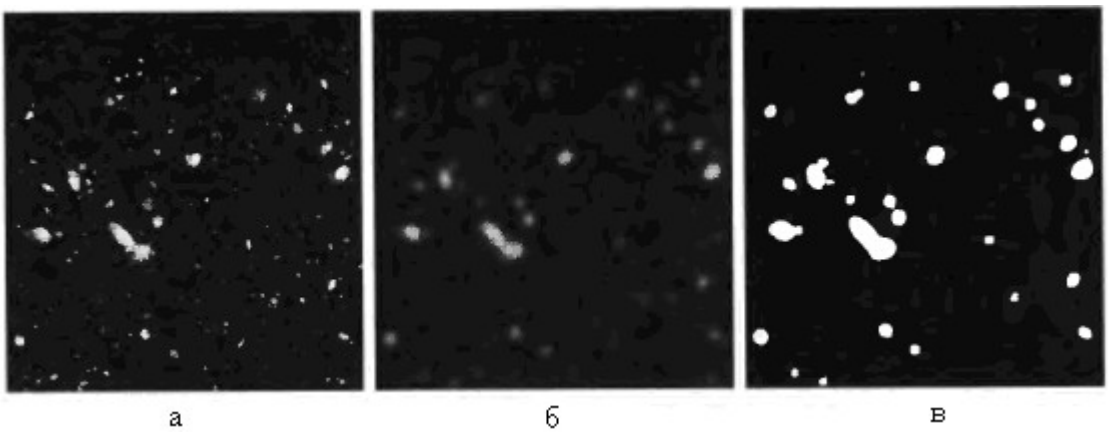


Рис.1.12. а – Зображення, отримане космічним телескопом «Хаббл»; б – зображення, оброблене маскою, що згладжує, розміром 15*15 елементів; в – результат застосування порогового виявлення до зображення (б) з рівнем порога 25% від найбільшої яскравості

Питання

1. Що таке цифрова обробка зображення?
2. Формальне представлення цифрового зображення.
3. Що є результатом дискретизації й квантування неперервного сигналу?
4. Як визначається функція градаційного перетворення зображення? Навести приклади функцій градаційного перетворення.
5. Як відбувається поліпшення контрастів цифрових зображень за допомогою степеневих перетворень?
6. Що називається гістограмою цифрового зображення? Поняття нормалізованої гістограми.
7. Поняття просторової фільтрації. Лінійні й нелінійні фільтри.

Тема 2. ПЕРЕТВОРЕННЯ ФУРЬЄ

План

1. Попередні зауваження
2. Визначення системи ортогональних функцій. Система ортонормованих функцій
3. Тригонометричні системи ортогональних функцій
4. Визначення ряду Фур'є по ортогональній системі функцій
5. Перетворення Фур'є й частотна область

1. Попередні зауваження

Головне наукове досягнення французького математика Жана Батисту Фур'є полягає, по суті, у наступному. Він показав, що будь-яка періодична функція може бути представлена у вигляді суми синусів і/або косинусів різних аргументів, помножених на деякі коефіцієнти, тобто у вигляді ряду Фур'є. Складність поведінки функції при цьому не має ніякого значення. Якщо тільки функція є періодичною й задовольняє деяким математичним умовам, вона може бути представлена у вигляді вищевказаної суми. Таким чином, простою мовою можна сказати, що будь-яка складна функція може бути представлена у вигляді суми простих (синусів і косинусів). Наприклад, нижня на рис.2.1 функція може бути представлена у вигляді суми чотирьох розташованих над нею функцій.

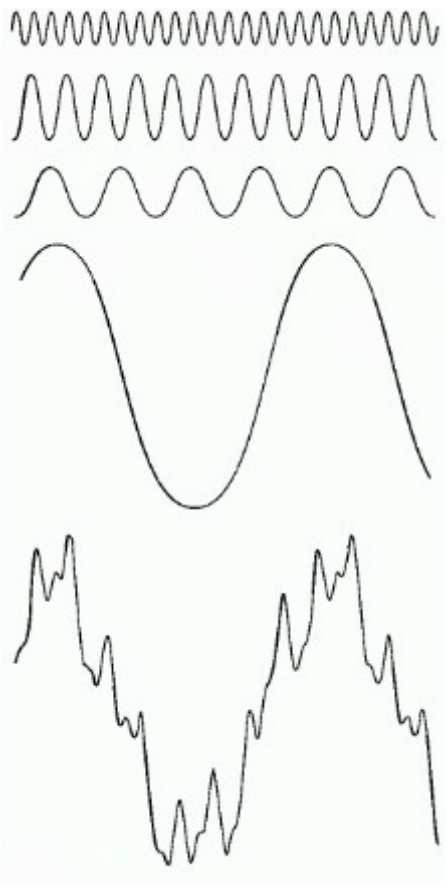


Рис.1.

Коли функція не є періодичною, вона може бути виражена у вигляді невласного інтеграла від синусів і/або косинусів, помножених на деяку вагову функцію. У такому випадку ми маємо справу з так званим перетворенням Фур'є.

Обидва представлення мають важливу характерну рису. Функція, задана як рядом, так і перетворенням Фур'є, може бути повністю, без втрати інформації, відновлена за допомогою деякої процедури відновлення. Ця властивість є однією з найбільш важливих властивостей розглянутих представлень, оскільки вона дозволяє працювати в «Фур'є-області», а потім повернутися у вхідну область визначення функції без втрати якої-небудь інформації про неї.

2.Визначення системи ортогональних функцій. Система ортонормованих функцій

Визначення 1. Система функцій $\varphi_1(x),\varphi_2(x),\ldots,\varphi_n(x),\ldots \quad x\in[a,b]$ називається *ортогональною*, якщо

$$\int_a^b \varphi_k(x)\varphi_l(x)=\begin{cases}0, & k\neq l\\ >0, & k=l\end{cases}. \tag{2.1}$$

Визначення 2. Число

$$\sqrt{\int_a^b f^2(x)dx} \tag{2.2}$$

будемо називати *нормою* $f(x)$ і позначати $\|f\|$.

Визначення 3. Ортогональна система функцій $\varphi_1(x),\varphi_2(x),\ldots,\varphi_n(x),\ldots \quad x\in[a,b]$ називається *ортонормальною*, якщо норма (2.2) для кожної з них: $\|\varphi_k(x)\|=1$ для $\forall k\in \mathrm{N}$.

Зауваження 1. Будь-яку ортогональну систему можливо зробити ортонормальною, розділивши кожну функцію на її норму.

3.Тригонометричні системи ортогональних функцій

Приклад 1. Система функцій

$$1,\cos x,\sin x,\cos 2x,\sin 2x,\ldots,\cos nx,\sin nx,\ldots \tag{2.3}$$

є ортогональною на $[-\pi,\pi]$. Для доказу цього треба перевірити виконання умови (2.1):

$$\int_{-\pi}^{\pi}\sin nx\sin mx\,dx=\frac{1}{2}\int_{-\pi}^{\pi}\big(\cos(n-m)x-\cos(m+n)x\big)=0 \text{ для } \forall n,m\in\mathrm{N};$$

$$\int_{-\pi}^{\pi}\cos nx\cos mx\,dx=\frac{1}{2}\int_{-\pi}^{\pi}\big(\cos(n-m)x+\cos(m+n)x\big)=0 \text{ для } \forall n,m\in\mathrm{N};$$

$$\int_{-\pi}^{\pi}\sin nx\cos mx\,dx=\frac{1}{2}\int_{-\pi}^{\pi}\big(\sin(n+m)x+\sin(n-m)x\big)dx=$$

$$=\frac{1}{2}\left(\frac{1}{n+m}\left(-\cos(n+m)x-\frac{1}{n-m}\cos(n-m)x\right)\right)\Bigg|_{-\pi}^{\pi}=0 \text{ для } \forall n,m\in\mathrm{N};$$

$$\int_{-\pi}^{\pi}\cos nx\,dx=0;\ \int_{-\pi}^{\pi}\sin nx\,dx=0 \text{ для } \forall n\in\mathrm{N};$$

$$\int_{-\pi}^{\pi}\cos^2 nx\,dx=\int_{-\pi}^{\pi}\frac{1+\cos 2nx}{2}dx=\left(\frac{1}{2}x+\frac{1}{2}\cdot\frac{1}{2n}\sin 2nx\right)\Bigg|_{-\pi}^{\pi}=\pi=\|\cos nx\|^2 \text{ для } \forall n\in\mathrm{N};$$

$$\int_{-\pi}^{\pi}\sin^2 nx\,dx=\int_{-\pi}^{\pi}\frac{1-\cos 2nx}{2}dx=\left(\frac{1}{2}x-\frac{1}{2}\cdot\frac{1}{2n}\sin 2nx\right)\Bigg|_{-\pi}^{\pi}=\pi=\|\sin nx\|^2 \text{ для } \forall n\in\mathrm{N};$$

$$\int_{-\pi}^{\pi} 1^2 dx = 2\pi = \|1\|^2 .$$

Таким чином, подана система (2.3) ортогональна.

Зауваження 2. Розглянута система (2.3) буде ортогональною на будь-якому проміжку довжини 2π.

Приклад 2. Система функцій

$$1, \sin\frac{\pi x}{l}, \cos\frac{\pi x}{l}, \ldots, \sin\frac{n\pi x}{l}, \cos\frac{n\pi x}{l}, \ldots \tag{2.4}$$

ортогональна на $[-l, l]$ і на будь-якому сегменті довжини $2l$.

Приклад 3. Система функцій

$$1, \cos x, \cos 2x, \ldots, \cos nx, \ldots$$

і система функцій

$$\sin x, \sin 2x, \ldots, \sin nx, \ldots$$

ортогональні на $[0, \pi]$.

Приклад 4. Система функцій

$$1, \cos\frac{\pi x}{l}, \cos\frac{2\pi x}{l}, \ldots, \cos\frac{n\pi x}{l}, \ldots$$

і система функції

$$\sin\frac{\pi x}{l}, \sin\frac{2\pi x}{l}, \ldots, \sin\frac{n\pi x}{l}, \ldots$$

ортогональні на $[0, l]$.

Системи з прикладів 1, 2 називаються *основними тригонометричними системами*.

4. Визначення ряду Фур'є по ортогональній системі функцій

Нехай є $f(x)$ $x \in [a, b]$ і

$$f(x) = c_1\varphi_1(x) + c_2\varphi_2(x) + \ldots + c_n\varphi_n(x) + \ldots, \tag{2.5}$$

де $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x), \ldots$ - ортогональна система функцій на $[a, b]$. Домножимо (2.5) на $\varphi_k(x)$ і проінтегруємо:

$$\int_a^b f(x)\varphi_k(x)dx = c_1\int_a^b \varphi_1(x)\varphi_k(x)dx + \ldots + c_k\int_a^b \varphi_k^2(x)dx + \ldots + c_n\int_a^b \varphi_n(x)\varphi_k(x)dx + \ldots \tag{2.6}$$

Всі інтеграли в правій частині останньої рівності дорівнюють 0, крім k-го, завдяки ортогональності системи функцій $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x), \ldots$. Тоді (2.6) можна записати в вигляді:

$$\int_a^b f(x)\varphi_k(x)dx = c_k \int_a^b \varphi_k^2(x)dx = c_k \|\varphi_k\|^2 \ ,$$

звідки

$$c_k = \frac{1}{\|\varphi_k\|^2} \int_a^b f(x)\varphi_k(x)dx \tag{2.7}$$

Тому $\forall\ f(x) \in Q_{[a,b]}$ можна поставити в співвідношення ряд

$$c_1\varphi_1(x) + c_2\varphi_2(x) + \ldots + c_k\varphi_k(x) + \ldots \tag{2.8}$$

де c_k визначаються по формулі (2.7).

Ряд (2.8) називається рядом Фурьє для $f(x)$ по ортогональній системі $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x), \ldots$

Запишемо ряд Фурьє для $f(x)$ $x \in [-\pi, \pi]$ по ортогональній системі функцій $1, \cos x, \sin x, \cos 2x, \sin 2x, \ldots$

$$f(x) = a_0 \cdot 1 + \sum_1^\infty (a_k \cos kx + b_k \sin kx),$$

де

$$a_0 = \frac{1}{\|\varphi_0\|^2} \int_{-\pi}^{\pi} f(x) \cdot \varphi_0(x)dx = \frac{1}{\|1\|^2} \int_{-\pi}^{\pi} f(x)dx = \left[\|1\|^2 = \int_{-\pi}^{\pi} dx = 2\pi \right] = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x)dx \, ;$$

$$a_k = \frac{1}{\|\cos kx\|^2} \int_{-\pi}^{\pi} f(x) \cdot \cos kx dx = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos kx \, dx \, ;$$

$$b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin kx \, dx \, , \ \forall k \in \mathrm{N} \, .$$

Для $\forall\ l > 0$ розглянемо функцію $f(x)$ на $(-l, l)$. На цьому проміжку візьмемо ортогональну систему

$$1, \sin\frac{\pi x}{l}, \cos\frac{\pi x}{l}, \ldots, \sin\frac{\pi n x}{l}, \cos\frac{\pi n x}{l}, \ldots$$

$$f(x) = a_0 + \sum_1^\infty \left(a_k \cos\frac{k\pi x}{l} + b_k \sin\frac{k\pi x}{l} \right) \tag{2.9}$$

Для $\forall\ l$ отримаємо свій ряд Фурьє.

$$f(x) \sim c_1\varphi_1(x) + \ldots + c_n\varphi_n(x) + \ldots$$

де $$c_k = \frac{1}{\|\varphi_k\|^2}\int_a^b f(x)\varphi_k(x)dx .$$

$$\left\|\cos\frac{k\pi x}{l}\right\|^2 = \int_{-l}^{l}\cos^2\frac{k\pi x}{l}dx = \int_{-l}^{l}\frac{1+\cos\frac{2k\pi x}{l}}{2}dx = \left(\frac{1}{2}x + \frac{l}{2k\pi}\sin\frac{2k\pi x}{l}\right)\Bigg|_{-l}^{l} = l ,$$

$$\left\|\sin\frac{k\pi x}{l}\right\|^2 = l \quad , \quad \|1\|^2 = 2l .$$

Тоді

$$a_0 = \frac{1}{2l}\int_{-l}^{l} f(u)du , \quad a_k = \frac{1}{l}\int_{-l}^{l} f(u)\cos\frac{k\pi u}{l}du ; \quad b_k = \frac{1}{l}\int_{-l}^{l} f(u)\sin\frac{k\pi n}{l}du .$$

Підставимо a_k і b_k в ряд (2.9):

$$f(x) = \frac{1}{2l}\int_{-l}^{l} f(u)du + \frac{1}{l}\sum_{1}^{\infty}\left(cos\frac{k\pi x}{l}\int_{-l}^{l} f(u)cos\frac{k\pi u}{l}du + sin\frac{k\pi x}{l}\int_{-l}^{l} f(u)cos\frac{k\pi u}{l}du \right)$$

5. Перетворення Фур'є й частотна область

Пряме перетворення Фур'є $F(u)$ неперервної функції однієї змінної $f(x)$ визначається рівністю:

$$F(u) = \int_{-\infty}^{\infty} f(x)e^{-i2\pi ux}dx .$$

По заданому перетворенню Фур'є $F(u)$ можна відновити вхідну функцію $f(x)$ за допомогою ***зворотного перетворення Фур'є***:

$$f(x) = \int_{-\infty}^{\infty} F(u)e^{i2\pi ux}du .$$

Ці перетворення становлять пару перетворень Фур'є, а вхідні в них функції утворюють ***Фур'є-пару***.

Для функції двох змінних $f(x,y)$ пряме перетворення Фур'є $F(u,v)$:

$$F(u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)e^{-i2\pi(ux+vy)}dxdy ,$$

Зворотне:

$$f(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} F(u,v)e^{i2\pi(ux+vy)}dudv .$$

Перетворення Фур'є дискретної функції однієї змінної $f(x)$, $x = 0,1,...,M-1$, - ***дискретне перетворення Фур'є*** (ДПФ) - визначається рівністю:

$$F(u) = \frac{1}{M}\sum_{x=0}^{M-1} f(x)e^{-i2\pi ux/M} , \quad u = 0,1,2,....,M-1 .$$

Як і вхідна функція $f(x)$, Фур'є-образ $F(u)$ є дискретною величиною й містить таке ж число елементів.

Вхідна функція відновлюється за допомогою зворотного ДПФ:

$$f(x) = \sum_{u=0}^{M-1} F(u) e^{i 2\pi ux / M}, \quad x = 0,1,2,....,M-1.$$

Важлива особливість дискретних перетворень полягає в тому, що, на відміну від неперервного випадку, тут немає необхідності опікуватися про існування ДПФ і зворотного до нього. Дискретне перетворення Фур'є і зворотне для нього завжди існують.

Поняття частотної області прямо випливає з формули Ейлера:

$$e^{i\varphi} = \cos\varphi + i\sin\varphi.$$

Тоді

$$F(u) = \frac{1}{M} \sum_{x=0}^{M-1} f(x)\left(\cos\left(2\pi ux / M\right) - i\sin\left(2\pi ux / M\right)\right), \quad u = 0,1,2,....,M-1.$$

Таким чином, кожний елемент перетворення Фур'є (тобто значення $F(u)$ для кожного значення u) складається із суми за всіма значеннями функції $f(x)$. Значення функції $f(x)$, в свою чергу, множаться на синуси й косинуси різних частот. Область значень змінної u, на якій приймає свої значення функція $F(u)$, називається ***частотною областю***, оскільки значення змінної u визначають частоти доданків, що складають перетворення. (Значення змінної x також впливають на частоти, але оскільки по цій змінній проводиться додавання, цей вплив однаковий для всіх значень змінної u). Кожний з M елементів функції $F(u)$ называється ***частотним компонентом перетворення***.

Модулем або ***спектром*** Фур'є-перетворення називається величина:

$$\left|F(u)\right| = \left(\left[\mathrm{Re}(F(u))\right]^2 + \left[\mathrm{Im}(F(u))\right]^2\right)^{\frac{1}{2}},$$

Фазою або ***фазовим спектром***:

$$\phi(u) = arctg\left[\frac{\mathrm{Im}(F(u))}{\mathrm{Re}(F(u))}\right],$$

Енергетичним спектром називається:

$$P(u) = \left|F(u)\right|^2 = \left(\left[\mathrm{Re}(F(u))\right]^2 + \left[\mathrm{Im}(F(u))\right]^2\right).$$

Дискретне пряме й зворотне перетворення Фур'є допускає узагальнення на двовимірний випадок. Пряме ДПФ функції $f(x,y)$ (ЦЗ) розміром $M \times N$:

$$F(u,v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-i2\pi\left(ux/M + vy/N\right)}, \quad u = 0,1,2,....,M-1,\ v = 0,1,2,....,N-1.$$

Зворотне ДПФ:

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{i2\pi(ux/M+vy/N)},\quad x=0,1,2,....,M-1,\ y=0,1,2,....,N-1.$$

Змінні u,v називаються ***частотними змінними***, змінні x,y - ***просторовими змінними*** або змінними зображення.

Фур'є-спектр, фаза, енергетичний спектр визначаються аналогічно одновимірному випадку:

$$|F(u,v)|=\left(\left[\mathrm{Re}(F(u,v))\right]^2+\left[\mathrm{Im}(F(u,v))\right]^2\right)^{\frac{1}{2}},$$

$$\phi(u,v)=arctg\left[\frac{\mathrm{Im}(F(u,v))}{\mathrm{Re}(F(u,v))}\right],$$

$$P(u,v)=|F(u,v)|^2=\left(\left[\mathrm{Re}(F(u,v))\right]^2+\left[\mathrm{Im}(F(u,v))\right]^2\right).$$

Значення

$$F(0,0)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)$$

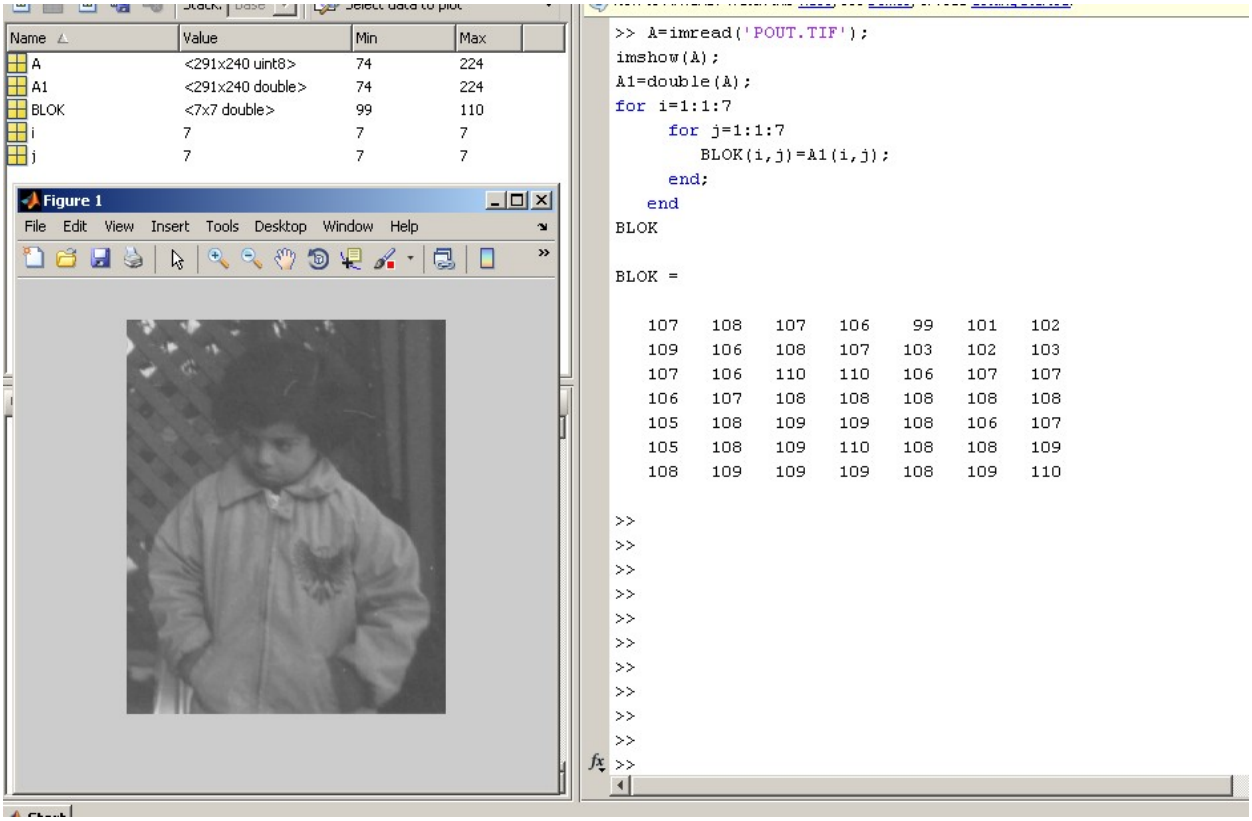
визначає середнє значення функції $f(x,y)$.

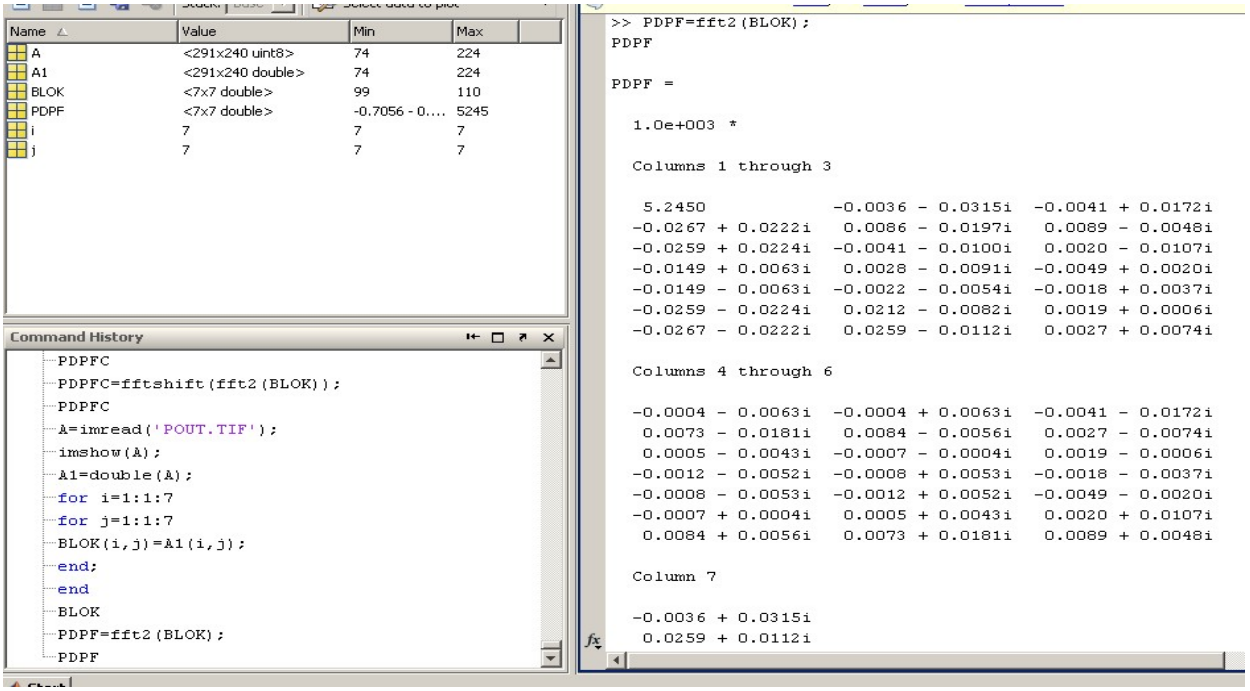
Звичайною практикою є множення вхідної функції (ЦЗ) на $(-1)^{x+y}$ перед обчисленням перетворення Фур'є (центрування спектру). Можна показати, що

$$\mathfrak{F}\left(f(x,y)(-1)^{x+y}\right)=F\left(u-M/2,v-N/2\right),$$

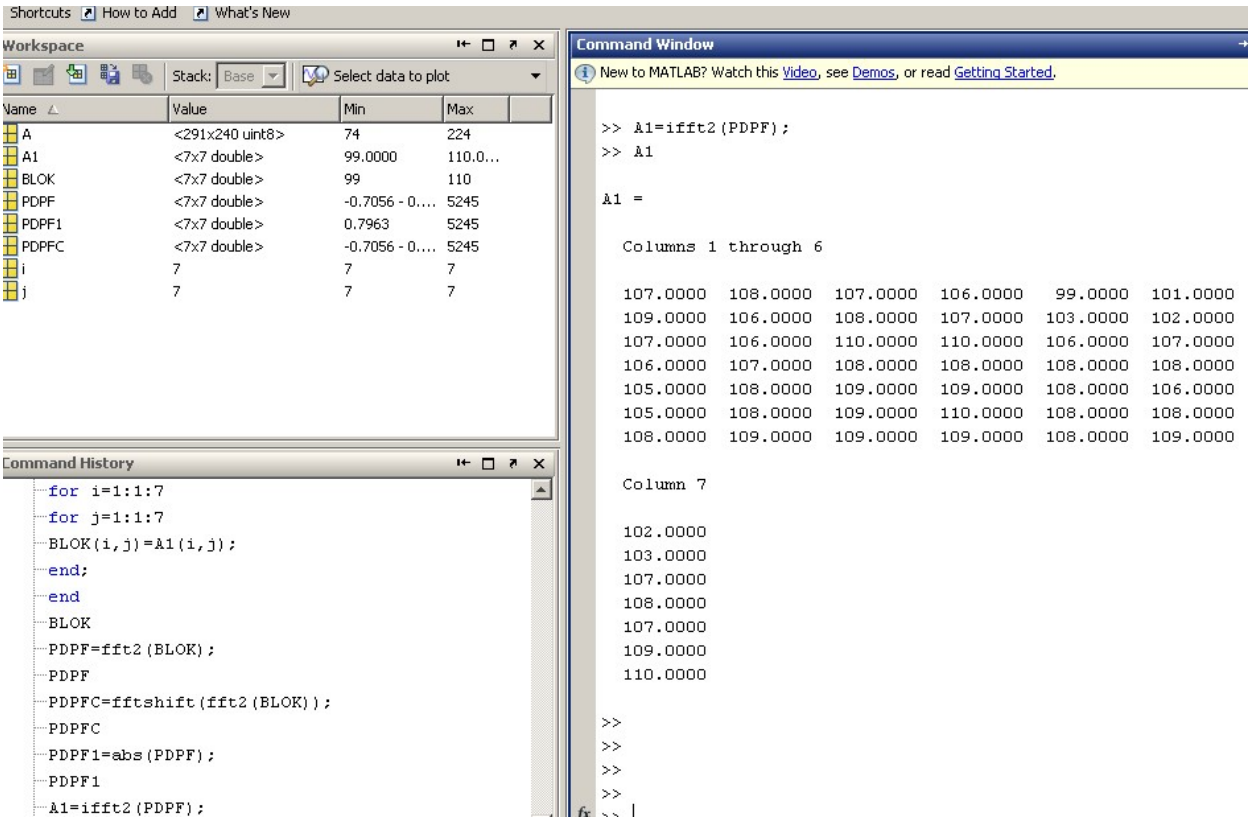
де $\mathfrak{F}$ – позначає перетворення Фур'є свого аргументу. Ця рівність означає, що початок координат для фур'є-перетворення функції $f(x,y)(-1)^{x+y}$ (тобто та точка, де значення цього перетворення дорівнює $F(0,0)$) знаходиться в точці з координатами $u=M/2,v=N/2$. Інакше кажучи, множення функції $f(x,y)$ на величину $(-1)^{x+y}$ приводить до зсуву початку координат для її образа $F(u,v)$ в точку з частотними координатами $\left(M/2,N/2\right)$.

Далі продемонстрований результат обробки блоку цифрового зображення в середовищі Matlab.

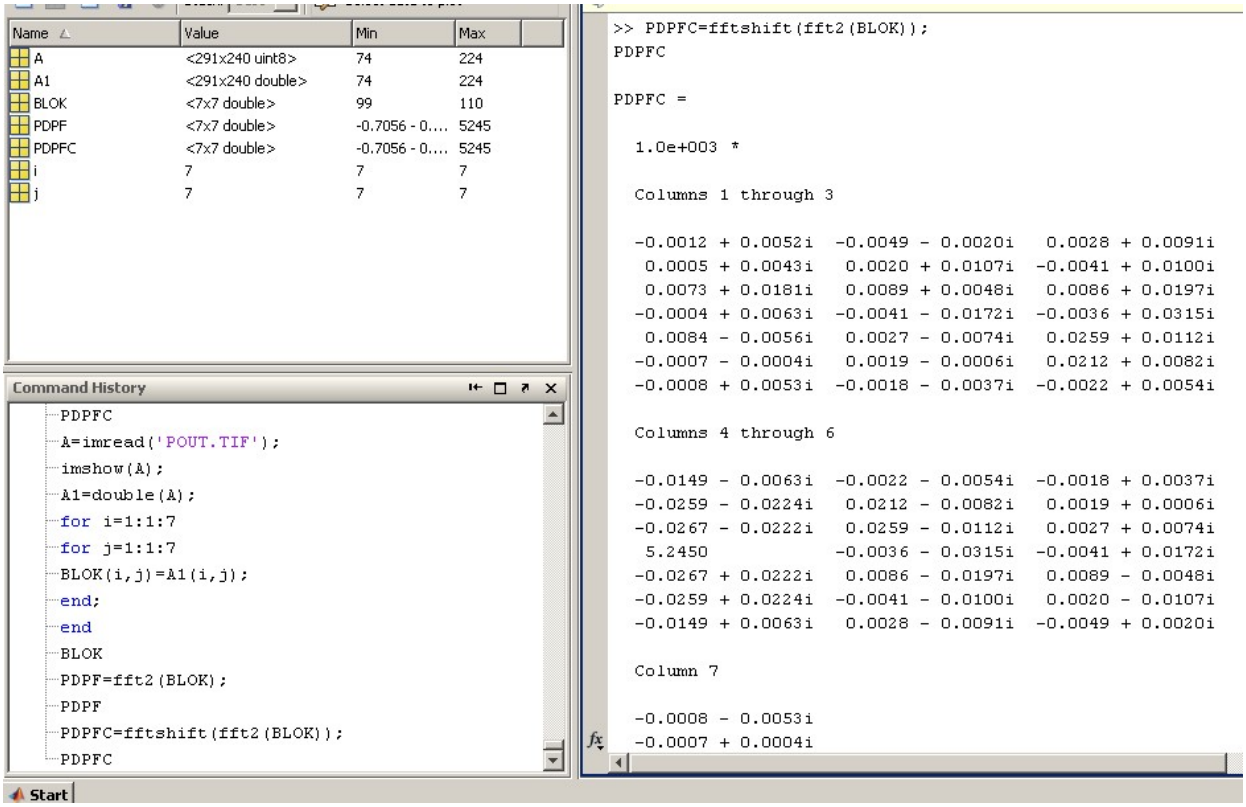




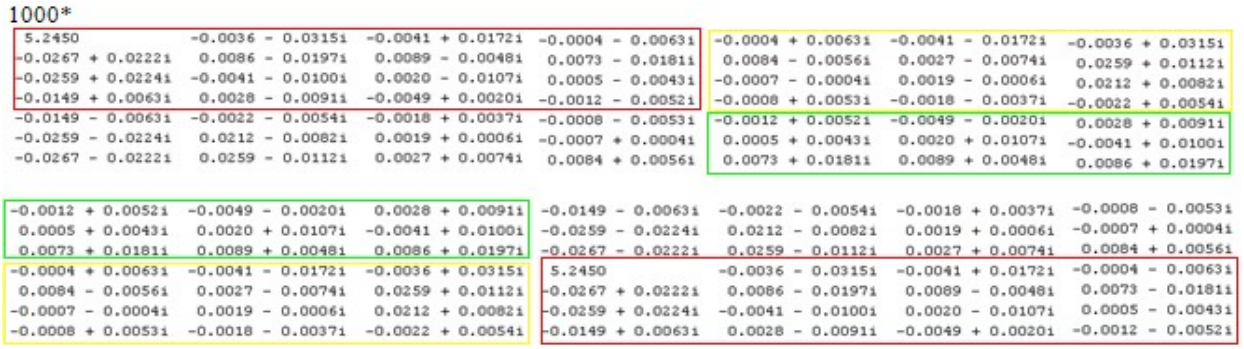
Зворотне перетворення Фур'є:



Центрування спектру



Для зручності порівняння матриці ДПФ і центрованого ДПФ разом:



Питання.

1. Яка система функцій називається ортогональной?
2. Що називається нормою $f(x)$?
3. Яка система функцій називається ортонормальною?
4. Як будь-яку ортогональну систему можна зробити ортонормальною?
5. Навести приклади ортогональних систем функцій. Довести, що наведені системи ортогональні.
6. Які системи функцій називаються основними тригонометричними системами?
7. Який ряд називається рядом Фурьє для $f(x)$ по ортогональній системі $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x), \ldots$? Навести приклади.

Тема 3. СТИСК ЦИФРОВИХ ЗОБРАЖЕНЬ

План

1. Поняття надмірності даних
2. Можливі способи стиску цифрового зображення
3. Відповідність між параметрами двовимірного сигналу в частотній області і області перетворення.
4. JPEG-стиск цифрового зображення.

1. Поняття надмірності даних

Термін ***стиск даних*** означає зменшення обсягу даних, використовуваного для представлення певної кількості інформації. При цьому між поняттями ***дані*** й ***інформація*** існують чіткі відмінності. Дані є тим засобом, за допомогою яких інформація передається, і для представлення одної кількості інформації може бути використана різна кількість даних. Це має місце в тому випадку, наприклад, коли дві різні людини, один - багатослівний, інший - лаконічний, розповідають одну й ту саму історію. У цьому випадку інформацією є факти, про які йде мова, слова - даними, що використовуються для викладу інформації. У випадку першого оповідача говорять про ***надлишковість даних***.

Надлишковість даних - центральне поняття цифрового стиску даних. Це вимірна математична категорія. Нехай n_1 і n_2 означають числа елементів - носіїв інформації - у двох наборах даних, що представляють одну й ту саму інформацію. Тоді відносна надлишковість даних R_D першого набору (n_1) стосовно другого набору (n_2) визначається як:

$$R_D = 1 - \frac{1}{C_R},$$

де C_R зазвичай називається ***коефіцієнтом стиску*** і є

$$C_R = \frac{n_1}{n_2}.$$

У задачі цифрового стиску зображень різняться й можуть бути використані три основні види надлишковості даних:

- ***Кодова*** надлишковість,
- ***Міжелементна***,
- ***Візуальна.***

Стиск даних досягається в тому випадку, коли скорочується або усувається надлишковість одного або декількох з вищевказаних видів.

Кодова надлишковість. Значна частка інформації про вид зображення може бути отримана на основі аналізу його гістограми значень яскравості. Гістограму зображення можна використовувати для побудови кодів, що зменшують необхідну кількість даних для представлення зображення (у випадку звичайного (або прямого) двійкового коду кожному інформаційному елементу або події (наприклад, значенню яскравості) дається одне з 2^m значень m-бітової двійкової послідовності). Однак, для представлення багатьох значень можна використовувати меншу кількість біт (наприклад, щоб представити 1 не треба мати 8 біт).

Міжелементна надлишковість. Міжелементна надлишковість пов'язана з міжелементними зв'язками усередині зображення. Оскільки значення будь-якого елемента ЦЗ може бути досить точно завбачине за значеннями його сусідів, то інформація, що міститься в окремому елементі, виявляється відносно малою. Більша частина внеску окремого елемента в зображення є надлишковою, вона може бути «вгадана» на основі значень сусідніх елементів. Для відображення подібного міжелементного зв'язку введені різні терміни, такі як ***просторова надлишковість***, ***геометрична надлишковість***, ***внутрікадрова надлишковість***. Об'єднанням їх усіх є термін міжелементна надлишковість.

Для зменшення межэлементной надмірності в зображенні двовимірний масив пікселів повинен бути перетворений у якийсь більш раціональний (але зазвичай «не візуальний») формат. Наприклад, для представлення зображення може бути використана різниця між сусідніми елементами.

Візуальна надлишковість. Сприймана оком яскравість залежить не тільки від кількості світла, що виходить із розглянутої області, але й від інших факторів. При звичайному візуальному сприйнятті частина інформації виявляється менш важливою, ніж інша. Таку інформацію називають ***візуально надлишковою***. Вона може бути вилучена без помітного погіршення візуальної якості зображення.

Найважливішою операцією під час оцифровки зорової інформації є ***квантування*** зображення. Квантування - відображення широкого (і, загалом кажучи, неперервного) діапазону вхідних значень в обмежений набір вихідних значень. Оскільки така операція необоротна (відбувається втрата візуальної інформації), то квантування є стиском із втратами.

2. Можливі способи стиску цифрового зображення

Стиск за допомогою використання малорангових апроксимацій зображення. Нехай F — матриця ЦЗ розміром $m \times n$ з елементами f_{ij}, $i = \overline{1,m}$, $j = \overline{1,n}$, ($m \geq n$).Для неї має місце сингулярне розкладання (SVD):

$$F = U\Sigma V^T, \qquad (3.1)$$

де U, V — матриці розміром $m \times n$ і $n \times n$ відповідно; $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$. При цьому U, V задовольняють співвідношенням: $U^T U = I$, $V^T V = I$, де I — одинична матриця відповідного розміру, тобто є ортогональними. Стовпці $u_1,...,u_n$ матриці U і $v_1,...,v_n$ матриці V називають відповідно лівими й правими сингулярними векторами матриці F, величини $\sigma_1,...,\sigma_n$ — *сингулярними числами* (СНЧ), а (σ_i, u_i, v_i) - *сингулярними трійками* F. (При $m < n$ розглядається SVD матриці F^T.)

Сингулярне розкладання (3.1) матриці F може бути представлено у формі зовнішніх добутків:

$$F = U\Sigma V^T = \sum_{i=1}^{n} \sigma_i u_i v_i^T \qquad (3.2)$$

У загальному випадку SVD матриці визначається неоднозначно. Назвемо вектор u ***лексикографічно додатним***, якщо його перший ненульовий компонент додатний, а SVD (3.1) нормальним, якщо стовпці матриці U лексикографічно додатні. Можна показати, що невироджена матриця має єдине нормальне SVD, якщо її СНЧ попарно різні. Таким чином, СНЧ і сингулярні вектори (СНВ), що отримані нормальним SVD, однозначно визначають матрицю ЦЗ.

Нехай F — симетрична $n \times n$-матриця, елементи якої $f_{ij} \in R$, $i, j = \overline{1,n}$, з власними значеннями (ВЗ) $\lambda_i \in R$, $i = \overline{1,n}$, і ортонормованими власними векторами (ВВ) u_i, $i = \overline{1,n}$, спектральне розкладання (СР) якої визначається відповідно до формули:

$$F = U\Lambda U^T \qquad (3.3)$$

де $\Lambda = diag(\lambda_1,...,\lambda_n)$ — матриця ВЗ; $U = [u_1,...,u_n]$ — матриця ВВ.

Розкладання (3.3), так само, як і (3.1), може бути представлене у формі зовнішніх добутків:

$$F = \sum_{i=1}^{n} \lambda_i u_i u_i^T \ .$$

В силу симетричності F її спектр, тобто множина всіх ВЗ, завжди дійсний. ВЗ, що є коренями характеристичного многочлена $\det(F - \lambda E) = 0$, визначаються однозначно, на відміну від СР (3.3).

За аналогією з нормальним SVD, СР назвемо нормальним, якщо елементи матриці Λ задовольняють співвідношенню: $|\lambda_1| \geq ... \geq |\lambda_n|$, а ВВ u_i, $i = \overline{1,n}$, лексикографічно додатні.

Теорема. Нехай F — невироджена симетрична $n \times n$-матриця, модулі ВЗ якої попарно різні. Тоді для неї існує єдине нормальне СР.

Як правило, матриця ЦЗ не задовольняє властивості: $F = F^T$. Поставимо у відповідність довільній F дві симетричні матриці A, B того ж розміру за наступним правилом:

$$F = \begin{pmatrix} a_{11}\ a_{12}\ a_{13}...a_{1n} \\ a_{21}\ a_{22}\ a_{23}...a_{2n} \\ a_{31}\ a_{32}\ a_{33}...a_{3n} \\ .....\\ a_{n1}\ a_{n2}\ a_{n3}...a_{nn} \end{pmatrix} \rightarrow A = \begin{pmatrix} a_{11}\ a_{12}\ a_{13}...a_{1n} \\ a_{12}\ a_{22}\ a_{23}...a_{2n} \\ a_{13}\ a_{23}\ a_{33}...a_{3n} \\ .....\\ a_{1n}\ a_{2n}\ a_{3n}...a_{nn} \end{pmatrix}, B = \begin{pmatrix} a_{11}\ a_{21}\ a_{31}...a_{n1} \\ a_{21}\ a_{22}\ a_{32}...a_{n2} \\ a_{31}\ a_{32}\ a_{33}...a_{n3} \\ .....\\ a_{n1}\ a_{n2}\ a_{n3}...a_{nn} \end{pmatrix}. \qquad (3.4)$$

Визначення. Матриця

$$F_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$$

називається ***малоранговою апроксимацією*** F.

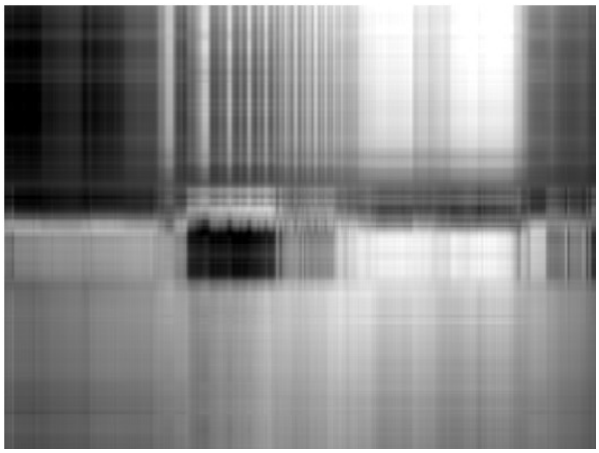
Визначення. Нехай $A = A^T$. Для матриці A побудоване нормальне СР (3.3). Матриця

$$A_k = \sum_{i=1}^{k} \lambda_i u_i u_i^T$$

називається ***малоранговою апроксимацією*** A.

Малорангові апроксимації матриці ЦЗ можуть бути використані для стиску зображення. Нехай матриця має розміри $m \times n$, тоді треба зберігати mn її елементів. З урахуванням того, що матриці оригінальних ЦЗ, як правило, мають значні розміри, актуальним є питання про те, чи можна скоротити цю кількість? Розглянемо як приклад ЦЗ на рис.3.1(а), розміри якого 480*640. Побудуємо SVD матриці ЦЗ. Розглянемо матрицю $F_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$, яка є наближенням до *F*, при цьому для відновлення матриці F_k необхідно лише $(m+n)k$ слів пам'яті, у яких зберігаються вектори $u_1,...,u_k$ і $\sigma_1 v_1,...,\sigma_k v_k$. Наближення вхідного ЦЗ для різних значень k наведені на рис.3.1(б,в,г)

а



б

в

г

Рис.3.1. Подане ЦЗ (а); результат стиску зображення шляхом використання апроксимації рангу $k=3$ (б); $k=65$ (в); (г) $k=110$

Для $k=110$ візуально ЦЗ не відрізняється від вхідного, однак виграш у пам'яті тут значний: для вхідного – 640*480=307200 слів пам’яті; при $k=110$ - (640+480)*110=123200, тобто приблизно в 3 рази.

Малорангові апроксимації ЦЗ роблять його стиск за рахунок обнуління високочастотних складових сигналу.

3. Відповідність між параметрами двовимірного сигналу в частотній області і області перетворення

Очевидно, існує певна відповідність між елементами енергетичного спектра й сингулярними трійками матриці вхідного цифрового сигналу.

Визначення. Назвемо

$$F_{k_d} = \sum_{i=k+1}^{n} \sigma_i u_i v_i^T$$

доповненням до апроксимації F_k,

$$S_k = \sigma_k u_k v_k^T$$

k **-ою** ***складовою*** зображення F.

На прикладі зображення CAMERAMAN розглянемо апроксимації різного рангу, а також доповнення до апроксимацій (рис.3.2). Результати візуально аналогічні результатам низькочастотної (рис.3.2(б,в)) і високочастотної фільтрації (рис.3.2(д,е)). Варіанти *а* і *г* (рис.3.2) зорово не відрізняються.

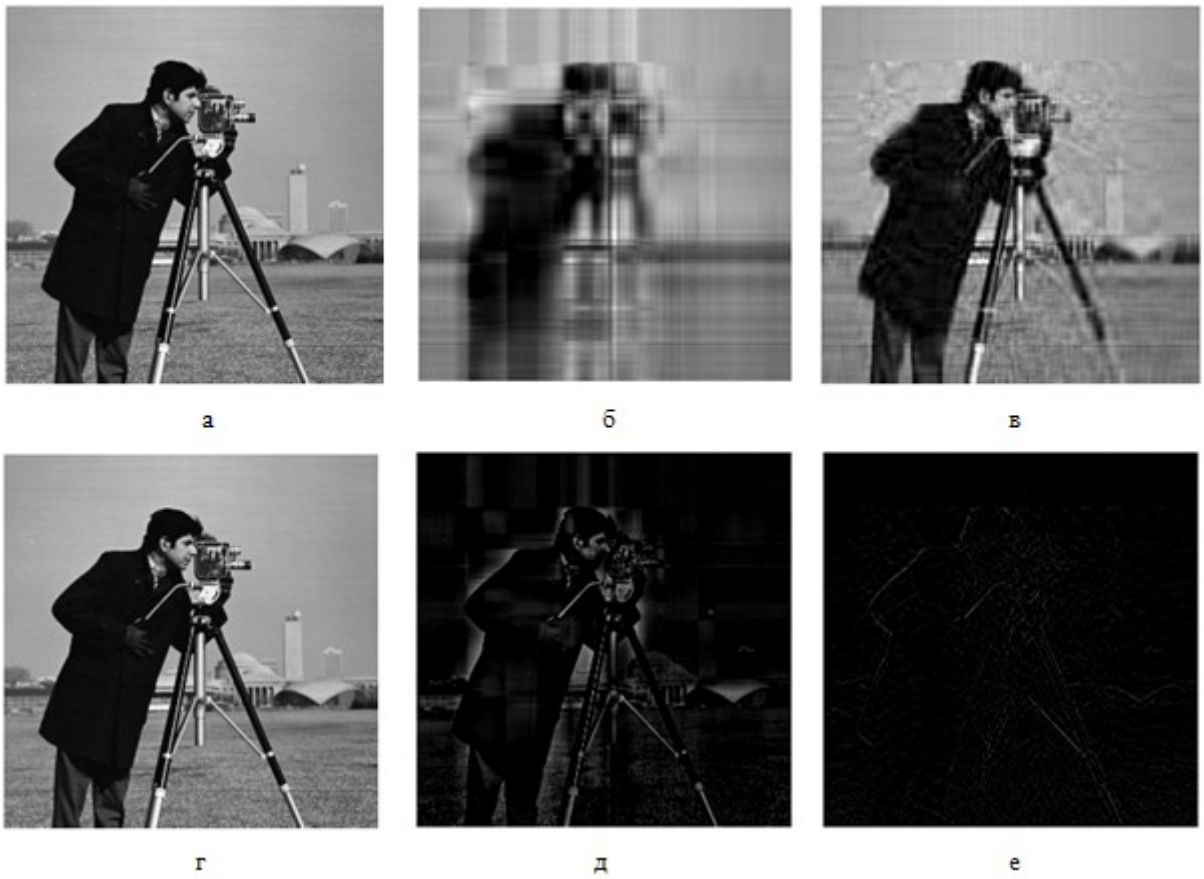


Рис.3.2. Зображення CAMERAMAN і його апроксимації: вхідне зображення (а); F_5 (б); F_{20} (в); F_{150} (г); F_{5_d} (д); F_{40_d} (е)

Виходячи з розглянутих результатів, висувається наступна

Гіпотеза: сингулярні трійки, що відповідають найбільшим СНЧ, відповідають, головним чином, низькочастотним, а найменшим - високочастотним складовим сигналу, яка повністю підтверджується на практиці.

4.JPEG-стиск цифрового зображення

Одним з найбільш повних і популярних стандартів стиску зображень є стандарт JPEG.

Сам процес стиску складається із трьох послідовних кроків:

а) Обчислення дискретного косинусного перетворення (ДКП) для матриць 8* 8-блоків, отриманих після стандартної розбивки матриці ЦЗ;

б) квантування коефіцієнтів ДКП;

в) кодування нерівномірним кодом.

Спочатку ЦЗ розбивається на окремі блоки розміром 8*8 елементів, які обробляються послідовно зліва направо і зверху вниз. Обробка кожного блоку починається зі зсуву по яскравості значень усіх його 64 елементів, що досягається відніманням величини 2^{n-1}, де 2^n - максимальне число рівнів яскравості. Потім обчислюється двовимірне ДКП елементів блоку. Отримані значення коефіцієнтів квантуються відповідно до формули:

$$\overline{T}(u,v) = round\left(\frac{T(u,v)}{Z(u,v)}\right),$$

де $\overline{T}(u,v)$ - результат квантування значень коефіцієнта ДКП $T(u,v)$, а $Z(u,v)$ - відповідний елемент матриці коефіцієнтів квантування:

$$Z = \begin{pmatrix} Z(1,1) & Z(1,2) & \dots & Z(1,8) \\ Z(2,1) & Z(2,2) & \dots & Z(2,8) \\ \dots & \dots & \dots & \dots \\ Z(8,1) & Z(8,2) & \dots & Z(8,8) \end{pmatrix}.$$

(Необхідно відзначити, що перед тим, як квантовані коефіцієнти ДКП $\overline{T}(u,v)$ можуть бути піддані зворотному ДКП для відновлення блоку зображення, вони повинні бути помножені на $Z(u,v)$:

$$\overline{\overline{T}}(u,v) = \overline{T}(u,v)Z(u,v). \qquad (3.5)$$

Очевидно, що зворотне перетворення отриманих значень $\overline{\overline{T}}(u,v)$ дасть у результаті наближення блоку зображення, що відновлюється).

Відквантовані значення коефіцієнтів переупорядковуються зигзаг-перетворенням згідно:

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

де показана черговість, у якій вибираються коефіцієнти. Результатом є одномірна послідовність квантованих коефіцієнтів.

Одномірний масив, отриманий після зигзаг-перетворення, упорядковується по зростанню просторової частоти, при цьому, як правило, виникають довгі послідовності нулів, що ефективно використовується процедурою Jpeg-кодування. Рекомендована JPEG-матриця квантування має такий вигляд:

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Приклад. *Послідовне кодування й декодування JPEG*. Розглянемо стиск і відновлення наступного блоку 8*8 елементів згідно зі стандартом послідовного кодування JPEG:

52	55	61	66	70	61	64	73
63	59	66	90	109	85	69	72
62	59	68	113	144	104	66	73
63	58	71	122	154	106	70	69
67	61	68	104	126	88	68	70
79	65	60	70	77	68	58	75
85	71	64	59	55	61	65	83
87	79	69	68	65	76	78	94

Вхідні пікселі можуть мати 256 або 2^8 рівнів яскравості, так що процес кодування починається зі зсуву діапазону значень - віднімання зі значень пікселів величини 2^7 або 128. У результаті виходить масив:

−76	−73	−67	−62	−58	−67	−64	−55
−65	−69	−62	−38	−19	−43	−59	−56
−66	−69	−60	−15	16	−24	−62	−55
−65	−70	−57	−6	26	−22	−58	−59
−61	−67	−60	−24	−2	−40	−60	−58
−49	−63	−68	−58	−51	−65	−70	−53
−43	−57	−64	−69	−73	−67	−63	−45
−41	−49	−59	−60	−63	−52	−50	−34

який після прямого ДКП буде мати вигляд:

–415	–29	–62	25	55	–20	–1	3
7	–21	–62	9	11	–7	–6	6
–46	8	77	–25	–30	10	7	–5
–50	13	35	–15	–9	6	0	3
11	–8	–13	–2	–1	1	–4	1
–10	1	3	–3	–1	0	2	–1
–4	–1	2	–1	2	–3	1	–2
–1	–1	–1	–2	–1	–1	0	–1

Якщо для квантування отриманих даних використовується наведена вище матриця квантування, то після квантування коефіцієнти будуть мати вид:

–26	–3	–6	2	2	0	0	0
1	–2	–4	0	0	0	0	0
–3	1	5	–1	–1	0	0	0
–4	1	2	–1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Процедура квантування дає значне число нульових елементів. Після того, як коефіцієнти переупорядковані відповідно до зигзаґ перетворення, вийде наступний масив:

(-26 -3 1 -3 -2 -6 2 -4 1 -4 1 1 5 0 2 0 0 -1 2 0 0 0 0 0 -1 -1 КБ)

Кодове слово КБ означає кінець блоку, указує на те, що всі коефіцієнти, що залишилися в переупорядкованій послідовності, дорівнюють 0. Для кодування отриманого масиву використовуються стандартні коди Хаффмана, що перетворять масив у неперервний потік біт.

При відновленні стисутого JPEG-блоку декодер у першу чергу повинен з неперервного потоку біт відтворити отквантовані коефіцієнти ДКП. Оскільки послідовність двійкових кодів Хаффмана є такою, що однозначно декодується, цей крок легко реалізується за допомогою табличного перетворення. Після множення на коефіцієнти квантування, згідно (3.5), одержимо масив:

–416	–33	–60	32	48	0	0	0
12	–24	–56	0	0	0	0	0
–42	13	80	–24	–40	0	0	0
–56	17	44	–29	0	0	0	0
18	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Повністю відновлений блок виходить після виконання зворотного ДКП отриманого масиву:

−70	−64	−61	−64	−69	−66	−58	−50
−72	−73	−61	−39	−30	−40	−54	−59
−68	−78	−58	−9	13	−12	−48	−64
−59	−77	−57	0	22	−13	−51	−60
−54	−75	−64	−23	−13	−44	−63	−56
−52	−71	−72	−54	−54	−71	−71	−54
−45	−59	−70	−68	−67	−67	−61	−50
−35	−47	−61	−66	−60	−48	−44	−44

і зворотного зсуву діапазону значень на $+2^7$=+128. В результаті отримаємо:

58	64	67	64	59	62	70	78
56	55	67	89	98	88	74	69
60	50	70	119	141	116	80	64
69	51	71	128	149	115	77	68
74	53	64	105	115	84	65	72
76	57	56	74	75	57	57	74
83	69	59	60	61	61	67	78
93	81	67	62	69	80	84	84

Усі відмінності значень елементів вхідного й відновленого блоків виникають внаслідок самої природи стиску із втратами, що є суттю JPEG-процедур стиску й відновлення. У даному прикладі помилки відновлення знаходяться у діапазоні від -14 до 11 і розподілені в такий спосіб:

−6	−9	−6	2	11	−1	−6	−5
7	4	−1	1	11	−3	−5	3
2	9	−2	−6	−3	−12	−14	9
−6	7	0	−4	−5	−9	−7	1
−7	8	4	−1	11	4	3	−2
3	8	4	−4	2	11	1	1
2	2	5	−1	−6	0	−2	5
−6	−2	2	6	−4	−4	−6	10

Характерні риси сингулярних чисел блоків матриці цифрового зображення при Jpeg-стиску.

Нехай вхідне ЦЗ в градаціях сірого, що зберігається в деякому форматі без втрат, наприклад, у форматі TIF, матриця якого F має розміри $n \times m$, розбивається стандартним чином на блоки 8×8. Якщо для кожного блоку A ЦЗ визначити множину усіх СНЧ (сингулярний спектр), то виявляється, що в середньому лише менш 1% від загального числа блоків (ЗЧБ) мають нульові СНЧ.

Даний факт не випадковий. Ранг будь-якої матриці визначається кількістю її ненульових СНЧ, а тому наявність нулів у сингулярному спектрі буде говорити про те, що число її лінійно незалежних рядків (стовпців) менше розміру. Однак, для довільного реального ЦЗ, навіть із врахуванням корельованості значень яскравості пікселів, імовірність того, що рядки (стовпці) чергового блоку виявляться лінійно залежними, невелика.

Квантування коефіцієнтів DCT, яке відбувається в процесі збереження ЦЗ у форматі JPEG (із втратами), є необерненою процедурою й приводить до деяких особливостей збурень СНЧ блоків.

Нехай вхідне ЦЗ піддалося Jpeg-стиску. Проведемо для нього операцію часткового відновлення (ЧВ), яка містить у собі: 1) ентропійне декодування; 2) множення отриманих коефіцієнтів на відповідні елементи масиву нормалізації (матриці квантування); 3) застосування зворотного DCT, але без наступного округлення.

В отриманої матриці практично всі блоки містять нульові СНЧ. Така ситуація закономірна. Після квантування й округлення коефіцієнтів DCT блоків багато з них, що відповідають високим і середнім частотам, обнуляться, залишаючись нулями після ЧВ, що, враховуючи відповідність між коефіцієнтами дискретного перетворення Фур'є й сингулярними трійками (σ_i, u_i, v_i) матриці зображення, де σ_i, u_i, v_i - СНЧ і лівий і правий СНВ, що йому відповідають, приведе до обнуління найменших (а можливо й середніх по величині) СНЧ матриць блоків.

Відзначимо, що, чим менше нульових СНЧ у розглянутому блоці, тим більше ліній контуру зображення він містить. Дійсно, наявність контурів у блоці говорить про значну високочастотну складову в сигналі, що відповідає цьому блоку. Тоді коефіцієнти DCT, що відповідають високим і середнім частотам, будуть порівняно великими й можуть залишитися ненульовими після квантування й ЧВ, а значить внесуть свій внесок не тільки в максимальні СНЧ.

Нехай вхідне зображення, що піддалося Jpeg-стиску, відновлюється повністю. Це означає, що після ЧВ усі значення яскравості пікселів округляються до цілих і вводяться в діапазон $[0, 255]$. Ця дія збурить матрицю зображення, отриману після ЧВ, певним чином зміниться кількість нульових СНЧ у блоках. Там, де після ЧВ не було елементів, значно менших 0 або більших 255, збурення матриці буде невеликим. Відповідно до співвідношення

$$\left|\sigma_i - \overline{\sigma}_i\right| \le \|E\|_2, \ \ i = \overline{1,n}, \tag{3.6}$$

Що має місце для довільної матриці, де $\sigma_i, \overline{\sigma}_i$ - СНЧ поданої і збуреної матриць відповідно, E - матриця збурення блоку, $\|\bullet\|_2$ - спектральна матрична норма, СНЧ є нечутливими до збурних дій. Якщо деякі з нульових СНЧ блоків матриці ЧВ-зображення стануть ненулями після повного відновлення, то їх значення будуть порівнянні з погрішністю округлення, що не характерно для блоків вхідного ЦЗ.

Питання

1. Що означає стиснення даних? Що таке надмірність даних?
2. Основні види надмірності даних.
3. Як реалізується стиск за допомогою квантування?
4. Що таке малорангова апроксимація зображення? Як реалізується стиск за допомогою використання малорангових апроксимацій зображення?
5. Що таке сингулярне розкладання матриці?
6. Що таке спектральне розкладання матриці?
7. Відповідність між параметрами цифрового зображення у просторовій та частотній областях.
8. Основні кроки JPEG-стиску цифрового зображення. Матриці квантування.
9. Характерні особливості сингулярних чисел блоків матриці цифрового зображення при стиску JPEG.
10. Часткове та повне відновлення цифрового зображення після стиснення

Тема 4. ОСНОВНІ ПОНЯТТЯ ЦИФРОВОЇ СТЕГАНОГРАФІЇ

План

1. Вступ.
2. Цифрова стеганографія. Предмет, термінологія, області застосування.
3. Структурна схема стеганосистеми.
4. Класифікація стеганосистем

1.Вступ

Завдання захисту інформації від несанкціонованого доступу вирішувалося за всіх часів протягом історії людства. Уже в прадавньому світі виділилося два основні напрямки розв'язку цього завдання, що існують і по сьогоднішній день: криптографія й стеганографія. Метою криптографії є приховання вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії приховується сам факт існування таємного повідомлення.

Слово «стеганографія» має грецьке коріння й буквально означає «тайнопис». Історично цей напрямок з'явився першим, але потім був витиснутий криптографією. Тайнопис здійснюється всілякими способами. Загальною рисою цих способів є те, що приховуване повідомлення або додаткова інформація (ДІ) вбудовується в деякий об'єкт, що не привертає увагу, який далі називається контейнером, або основним повідомленням (ОП). Результат такого вбудовування будемо називати стеганоповідомленням (СП), а сам процес вбудовування - стеганоперетворенням (СПр) контейнера. Потім стеганоповідомлення відкрито транспортується адресатові або зберігається в отриманому виді.

При використанні криптографії наявність шифрованого повідомлення сама по собі привертає увагу супротивників, при використанні стеганографії ж наявність прихованого зв'язку залишається непомітною.

Згідно із принципом Кергоффа, система захисту інформації повинна забезпечувати свої функції навіть при повній поінформованості супротивника про її структуру й алгоритмах функціонування; Уся таємність системи захисту переданих відомостей повинна полягати в ключі, тобто в попередньо (як правило) розділеному між адресатами фрагменті інформації.

Стеганографія - це наука, яка вивчає способи й методи приховування конфіденційної інформації, основною задачею якої є приховування самого факту існування секретних даних при їхній передачі, зберіганні або обробці. Під прихованням існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні наявності іншого (прихованого) повідомлення, але й взагалі неможливість виникнення будь-яких підозр на цей рахунок.

Розвиток засобів обчислювальної техніки в останнє десятиліття дав новий поштовх для розвитку *комп'ютерної стеганографії*. З'явилося багато нових областей застосування. Повідомлення вбудовують тепер у цифрові дані, які, як правило, мають аналогову природу. Це - аудіо, зображення, відео. Відомі також пропозиції по вбудовуванню інформації в текстові файли й в файли програм.

Існують два основні напрямки в комп'ютерній стеганографії: пов'язаний із цифровою обробкою сигналів і не пов'язаний. В останньому випадку повідомлення можуть бути вбудовані в заголовки файлів, заголовки пакетів даних. Цей напрямок має обмежене застосування у зв'язку з відносною легкістю розкриття й/або знищення прихованої інформації. Більшість поточних досліджень в області стеганографії так чи інакше пов'язані із цифровою обробкою сигналів. Це дозволяє говорити про цифрову стеганографію, яка й розглядається далі.

Розвиток стеганографії сьогодні відбувається стрімко й багатогранно. Можна виділити дві причини популярності досліджень в області стеганографії в цей час: обмеження на використання криптозасобів у ряді країн світу (у тому числі, в Україні) і поява проблеми захисту прав власності на інформацію, представлену в цифровому виді.

Перша причина спричинила велику кількість досліджень у дусі класичної стеганографії (тобто приховування факту передачі інформації), друга - ще більш численні роботи в області так званих водяних знаків. *Цифровий водяний знак* (ЦВЗ) – спеціальна мітка, впроваджувана в зображення або інший цифровий сигнал з метою тим або іншим способом контролювати його використання.

Для конкретності далі будемо розглядати цифрові зображення (ЦЗ).

2. Цифрова стеганографія. Предмет, термінологія, області застосування

Цифрова стеганографія як наука народилася буквально в останні роки; Як відносно молода наука вона ще не має загальновизнаної класифікації й навіть термінології, Однак можна запропонувати наступну класифікацію напрямків, які містить у собі стеганографія:

- вбудовування інформації з метою її прихованої передачі (класична стеганографія);
- вбудовування цифрових водяних знаків (watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting) - «відбитків пальців»;
- вбудовування заголовків (captioning).

Класична стеганографія зазвичай спрямована на організацію прихованого каналу зв'язку в каналі загального користування й до недавнього часу залучала до себе основну увагу фахівців. Однак на сьогоднішній день у зв'язку з бурхливим розвитком інформаційних технологій, комп'ютерної техніки, використовуваної повсюдно, перевводу левиної частки інформації в цифрову форму акценти трохи змістилися, принаймні, як можна судити по публікаціях у відкритій пресі: основна увага приділяється другому з перерахованих напрямків стеганографії.

ЦВЗ можуть застосовуватися, в основному, для захисту від копіювання й несанкціонованого використання. У зв'язку з розвитком технологій мультимедіа гостро встало питання захисту авторських прав і інтелектуальної власності, представленої в цифровому виді. Прикладами можуть бути фото, аудіо й відеозаписи й т.д. Переваги, які дають представлення й передача повідомлень у цифровому виді, можуть виявитися перекресленими легкістю, з якої можливо їх злодійство або модифікація. Тому розробляються різні заходи захисту інформації, організаційного й технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації й полягає у вбудовуванні в об'єкт, що захищається, невидимих (видимих) міток - ЦВЗ. Розробки в цій області ведуть в усьому світі. Оскільки методи ЦВЗ почали розроблятися зовсім недавно (першою статтею на цю тему була робота 1989 р.), то тут є багато неясних проблем, що вимагають свого рішення. Назву ці методи отримали від усім відомого способу захисту цінних паперів, у тому числі й грошей, від підробки. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їхню коректність. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або яку-небудь керуючу інформацію. Найбільш підходящими об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, файли аудіо й відеоданих.

Технологія вбудовування ідентифікаційних номерів виробників має багато спільного з технологією ЦВЗ. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний номер, що вбудовується (звідси й назва - дослівно «відбитки пальців»). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то «відбитки пальців» швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту й т.д. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдине застосування стеганографії, де в явному виді відсутній потенційний порушник.

Двома основними вимогами до стеганоперетворення є:

- непомітність - надійність сприйняття стеганоповідомлення;
- стійкість до різного роду спотворень.

Слово «непомітність» має на увазі обов'язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що пред'являє до системи передачі вимоги, що досить важко формалізувати.

Якими б не були різними напрямки стеганографії, пропоновані ними вимоги багато в чому співпадають. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВЗ полягає в тому, що в першому випадку порушник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування знають. Більше того, у порушника на законних підставах може бути обладнання виявлення ЦВЗ (наприклад, у складі DVD-програвача).

3. Структурна схема стеганосистеми

Завдання вбудовування й виділення повідомлень із іншої інформації виконує стеганосистема, яка, як правило, складається з наступних основних елементів, представлених на рис.4.1:

- попередній кодер - пристрій, призначений для перетворення приховуваного повідомлення (конфіденційної інформації (КІ), ЦВЗ) до виду, зручного для вбудовування в контейнер;
- кодер - пристрій, призначене для здійснення вкладення додаткової інформації в контейнер з урахуванням його моделі (його особливостей);
- пристрій виділення вбудованого повідомлення;
- детектор – пристрій, призначений для визначення наявності вкладеної ДІ;
- декодер – пристрій, що відновлює конфіденційну інформацію. Цей вузол може бути відсутнім.

Дані, що містять приховане повідомлення, можуть піддаватися навмисним атакам або випадковим перешкодам, зокрема, у каналі атаки.

Перш, ніж здійснити вкладення КІ, ЦВЗ у контейнер, КІ (ЦВЗ) повинна бути перетворена до деякого підходящого виду, наприклад, якщо в якості контейнера виступає зображення, то й перетворена в попередньому кодері КІ (ЦВЗ) найчастіше представляється як двовимірний масив біт. Обробка в попередньому кодері виконується з використанням ключа *K* для забезпечення таємності вбудовування. Результатом попереднього кодування є додаткова інформація, що представляє із себе, як правило (але не обов'язково), бітову послідовність. Далі ДІ «вбудовується» у контейнер, наприклад, шляхом модифікації молодших значущих біт значень яскравості пікселів (у випадку цифрового зображення-контейнера). Цей процес можливий завдяки особливостям системи сприйняття людини: добре відомо, що зображення мають велику психовізуальну надлишковість; око людини подібне низькочастотному фільтру, що пропускає дрібні деталі. Особливо непомітні спотворення у високочастотній області зображень. Ці особливості людського зору використовуються, наприклад, при розробці алгоритмів стиску зображень і відео.

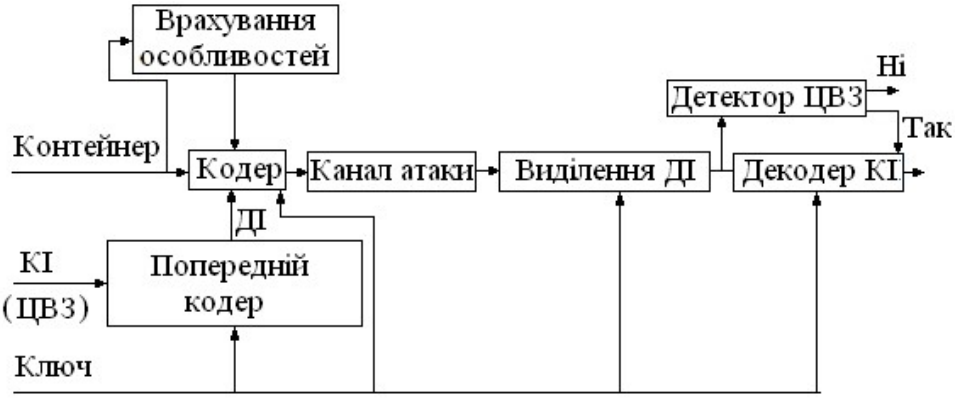


Рис.4.1. Схема типової стеганосистеми

Процес вбудови ДІ також повинен ураховувати властивості системи сприйняття людини. Стеганографія використовує наявну в сигналах психовізуальну надлишковість, але іншим, чим при стиску даних, образом. Наведемо простий приклад. Розглянемо півтонове зображення з 256 градаціями сірого. Добре відомо, що око людини не здатне помітити зміну молодшого значущого біта. Ще в 1989 році був отриманий патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біта. У цьому випадку детектор стего аналізує тільки значення цього біта для кожного пікселя, а око людини, навпаки, сприймає тільки старші 7 біт. Хоча даний метод простий у реалізації й ефективний, він не задовольняє деяким важливим вимогам, зокрема не забезпечує стійкість до атак проти вбудованого повідомлення.

У стегодетекторі відбувається виявлення ДІ в можливо зміненому зображенні. Ця зміна може бути обумовлена впливом помилок у каналі зв'язку, операцій обробки сигналу, навмисних атак порушників.

4. Класифікація стеганосистем

Залежно від того, яка інформація потрібно детектору для виявлення ДІ, стеганосистеми розподіляються на три класи:

- *відкриті*,
- *напівзакриті,*
- *закриті*.

Ця класифікація наведена в табл.4.1.

Таблиця 4.1. Класифікація стеганосистем

Класс стеганосистеми		Що потрібно детектору		Вихід детектора	
		Вхідний сигнал	Вхідна ДІ	Так/ні	ДІ
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Найбільше застосування мають відкриті стеганосистеми. Найбільшу стійкість стосовно зовнішніх впливів - закриті стеганосистеми I типу.

Класифікація стеганосистем потребує конкретизації поняття й типів контейнера. До кодера (рис.4.1) – це порожній контейнер, після нього – заповнений контейнер, або стеганоповідомлення (СП). СП повинно візуально не відрізнятися від порожнього контейнера при організації прихованого каналу зв'язку.

Розрізняють два основні типи контейнерів: *потоковий* і *фіксований*.

Потоковий контейнер являє собою послідовність біт, що безперервно подається; повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано й кілька повідомлень. Потоковий контейнер має велике практичне значення: наприклад, стегоприставка до звичайного телефону: під прикриттям звичайного, незначного телефонного переговору можна передавати іншу розмову, дані й інше, і, не знаючи секретного ключа, не можна не тільки довідатися про зміст прихованої передачі, але й сам факт її існування. Не випадково, що робіт, присвячених розробці стеганосистем з потоковим контейнером практично не зустрічається у відкритій пресі.

У *фіксованого* контейнера розміри й характеристики заздалегідь відомі, що дозволяє здійснювати вкладення даних оптимальним у деякому сенсі образом.

Контейнер може бути *обраним, випадковим або нав'язаним*. *Обраний контейнер* залежить від повідомлення, що вбудовується, а в граничному випадку є його функцією. Цей тип контейнера більше характерний для класичної стеганографії. *Нав'язаний контейнер* може з'явитися в сценарії, коли особа, що надає контейнер, підозрює про можливу приховану переписку й бажає запобігти її. На практиці ж найчастіше зустрічаються з *випадковим* контейнером.

Вбудовування повідомлення в контейнер проводиться з використанням ключа, одного або декількох. Приховувана інформація, як правило, вбудовується відповідно до ключа в ті відліки, спотворення яких не приводить до істотних спотворень контейнера. Ці відліки утворюють *стеганошлях*. Залежно від області застосування під істотним спотворенням можна розуміти спотворення, що приводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення факту наявності прихованого повідомлення після стеганоаналізу.

Захист цифрового контейнера від його несанкціонованого використання доцільно проводити з використанням ЦВЗ, які можуть бути трьох типів: робастні, хрупкі й напівхрупкі (semifragile), і використовуються залежно від переслідуваної мети.

Під робастністю ЦВЗ розуміється його стійкість до різного роду збурних дій на СП. Більшість досліджень у цьому напрямку стеганографії присвячено робастним ЦВЗ.

Хрупкі ЦВЗ руйнуються при незначній модифікації СП; вони застосовуються для автентифікації контейнера. Відмінність від засобів електронного цифрового підпису полягає в тому, що хрупкі ЦВЗ все-таки допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, тому що законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність від засобів електронного цифрового підпису полягає в тому, що хрупкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також вид і місце розташування цієї зміни, що робить їх кращими в умовах автентифікації контейнера.

Напівхрупкі ЦВЗ стійкі стосовно одних збурних дій і нестійкі стосовно інших. Загалом кажучи, усі ЦВЗ можуть бути віднесені до цього типу. Однак напівхрупкі ЦВЗ спеціально проектують так, щоб бути нестійкими стосовно певного роду операцій. Наприклад, вони можуть дозволяти виконувати стиск зображення, але забороняти вирізку з нього або вставку в нього фрагмента.

Питання

1. Що називається контейнером, стеганоповідомленням? Що має сенс використовувати як контейнер для організації стеганографічного каналу зв'язку? Чому?
2. Принцип Керхгоффа.
3. Що таке стеганографія, комп'ютерна стеганографія, цифрова стеганографія?
4. Які причини популярності досліджень у галузі стеганографії сьогодні?
5. Класифікація напрямків, які включає стеганографія.
6. Що таке цифровий водяний знак? Навіщо він використовується?
7. Дві основні вимоги до стеганографічного перетворення.
8. Структурна схема стеганосистеми.
9. Класифікація стеганосистем.
10. Визначення стеганошляху.
11. Що таке потоковий, фіксований контейнер? Переваги та недоліки.
12. Що таке обраний, випадковий нав'язаний контейнер? Переваги та недоліки.

Тема 5. ОРГАНІЗАЦІЯ ПРИХОВАНОГО КАНАЛУ ЗВ’ЯЗКУ

План

1. Вимоги, що висуваються при проектуванні стеганосистеми
2. Метод модифікації найменшого значущого біта, його переваги, недоліки
3. Граф цифрового зображення

1. Вимоги, що висуваються при проектуванні стеганосистеми

Для того, щоб стеганосистема була надійною, необхідно виконання при її проектуванні ряд вимог:

- Безпека системи повинна повністю визначатися таємністю ключа: порушник може повністю знати всі алгоритми роботи стеганосистеми й статистичні характеристики множин повідомлень і контейнерів, але це не дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері.
- Знання порушником факту наявності повідомлення в якому-небудь контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.
- Заповнений контейнер при організації прихованого каналу зв'язку повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здається, вбудовувати приховуване повідомлення у візуально незначущі області сигналу, однак, ці ж області використовують і алгоритми стиску. Тому, якщо зображення буде надалі зазнавати стиск, то приховане повідомлення може зруйнуватися, отже, біти ДІ доцільно вбудовувати у візуально значимі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів.
- Стеганосистема ЦВЗ повинна мати низьку ймовірність неправильного виявлення прихованого повідомлення в сигналі, який його не містить. У деяких додатках таке виявлення може привести до серйозних наслідків, наприклад, неправильне виявлення ЦВЗ на DVD-диску може викликати відмову від його відтворення плейєром.
- Повинна забезпечуватися необхідна пропускна спроможність (ця вимога актуальна, в основному, для стеганосистем прихованої передачі інформації).
- Стеганосистема повинна мати прийнятну обчислювальну складність реалізації.

До ЦВЗ пред'являються наступні вимоги:

- ЦВЗ повинен легко (в обчислювальному сенсі) витягатися законним користувачем.
- ЦВЗ повинен бути стійким або нестійким до навмисних і випадкових впливів (залежно від області застосування). Якщо ЦВЗ використовується для підтвердження оригінальності, то неприпустима зміна контейнера повинна приводити до руйнування ЦВЗ (хрупкий ЦВЗ); якщо ж ЦВЗ містить ідентифікаційний код, логотип фірми й таке інше, то він повинен зберегтися при максимальних спотвореннях контейнера, звичайно, що не приводять до істотних спотворень вхідного сигналу. Наприклад, у зображення можуть бути відредагована колірна гама або яскравість, в аудиозапису - посилене звучання низьких тонів і т.д. Крім того ЦВЗ повинен бути робастним стосовно аффінних перетворень зображення, тобто його поворотам, масштабуванню. При цьому треба розрізняти стійкість самого ЦВЗ і здатність декодера вірно його виявити. Скажемо, при повороті зображення ЦВЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатка, коли ЦВЗ повинен бути стійким стосовно одних перетворень і нестійким стосовно інших, наприклад, може бути дозволене копіювання зображення (ксерокс, сканер), але накладена заборона на внесення в нього яких-небудь змін.

2.Метод модифікації найменшого значущого біта

Молодший значущий біт (LSB) зображення містить в собі найменше інформації. Людина зазвичай не здатна помітити зміну в цьому біті. Фактично, він є шумом, тому його можна використовувати для вбудовування інформації. Таким чином, для півтонового зображення обсяг даних, що вбудовуються, може становити 1/8 обсягу контейнера.

Наприклад, у зображення розміром 512x512 можна вбудувати 32 кілобайта інформації. Якщо модифікувати два молодші біти (що також майже непомітно), то можна вбудувати вдвічі більший обсяг даних.

Переваги розглянутого методу полягають у його простоті й порівняно великому обсязі даних, що вбудовуються. Однак, він має серйозні недоліки: по-перше, приховане повідомлення легко зруйнувати; по-друге, не забезпечена таємність вбудовування інформації. Порушникові точно відоме місце розташування всього ЦВЗ (ДІ). Для подолання останнього недоліку було запропоновано вбудовувати ДІ (ЦВЗ) не в усі пікселі зображення, а лише в деякі з них, які визначаються за псевдовипадковим законом відповідно до ключа, відомого тільки законному користувачеві. Пропускна спроможність при цьому зменшується.

Розглянемо докладніше питання вибору пікселів зображення для вбудовування в них прихованого повідомлення.

Характер поведінки молодшого значущого біта зображень невипадковий. Приховуване повідомлення не повинно змінювати статистики зображення. Для цього, у принципі можливо, маючи велику кількістю незаповнених контейнерів, підшукати найбільш підходящий. Теоретично можливо знайти контейнер, що вже містить у собі наше повідомлення при даному ключі. Тоді змінювати взагалі нічого не треба, і розкрити факт передачі буде неможливо. Метод вибору підходящого контейнера вимагає виконання великої кількості обчислень і має малу пропускну спроможність.

У силу зазначених труднощів на практиці зазвичай обмежуються пошуком пікселів, модифікація яких не вносить помітних спотворень у зображення. Потім із цих пікселів відповідно до ключа вибираються ті, які будуть модифікуватися. Приховуване повідомлення шифрується із застосуванням іншого ключа. Цей етап може бути доповнений попередньою компресією для зменшення обсягу повідомлення.

3. Граф цифрового зображення

Розглянемо одну з можливостей організації визначення пікселів, модифікація яких не вносить помітних спотворень у зображення.

У якості контейнера будемо розглядати зображення; у якості математичної моделі вхідного зображення розглянемо не матрицю F, як це традиційно робиться, а побудований певним чином неорієнтований граф $G_F(X,E)$. Нехай F - $n \times n$-матриця зображення, що визначається функцією $f(x,y)$. Граф $G_F(X,E)$ будемо називати *графом зображення*, якщо

1) $|X| = n^2$, до того ж кожна вершина відповідає одному й тільки одному елементу матриці *F*;

2) ребро <*i, j*> належить множині E тоді й тільки тоді, коли вершини *i* і *j* графа $G_F(X,E)$ відповідають таким сусіднім елементам $F(k_i,m_i)$ і $F(k_j,m_j)$ матриці *F*, для яких

$$|F(k_i,m_i) - F(k_j,m_j)| > M,$$

де M – припустимий стрибок функції.

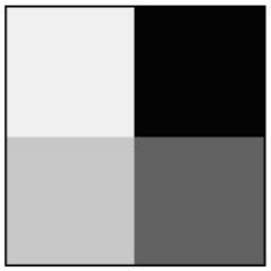


Рис. 5.1. Тестове ЦЗ

Для ілюстрації визначення розглянемо приклад. На рис.5.1 представлено зображення в градаціях сірого. Не обмежуючи спільності, для простоти припустимо, що розмір зображення 10x10 пікселів (n=10).

Матриця, що відповідає цьому зображенню, має вигляд:

$$F = \begin{pmatrix} 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 240 & 240 & 240 & 240 & 240 & 4 & 4 & 4 & 4 & 4 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \\ 200 & 200 & 200 & 200 & 200 & 98 & 98 & 98 & 98 & 98 \end{pmatrix}$$

Нумерацію графа проведемо в такий спосіб: елементу $F(i,j)$ матриці буде відповідати вузол графа з номером $(i-1)n+j$. Така нумерація зберігає наочність відповідності між матрицею й графом. Граф, що відповідає зображенню на рис.5.1, при M=30 представлений на рис. 5.2, при M=100 - на рис. 5.3 (вибір M для довільної $f(x,y)$ визначається залежно від виду самого зображення, від характеру заданих обмежень або експериментально) .

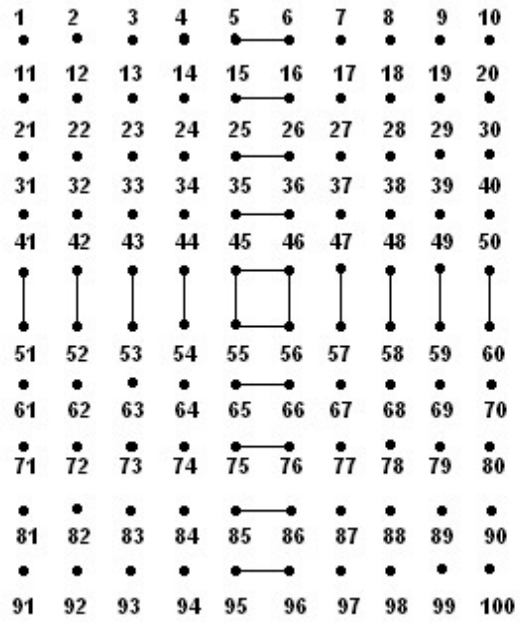


Рис.5.2. Граф ЦЗ (M=30)

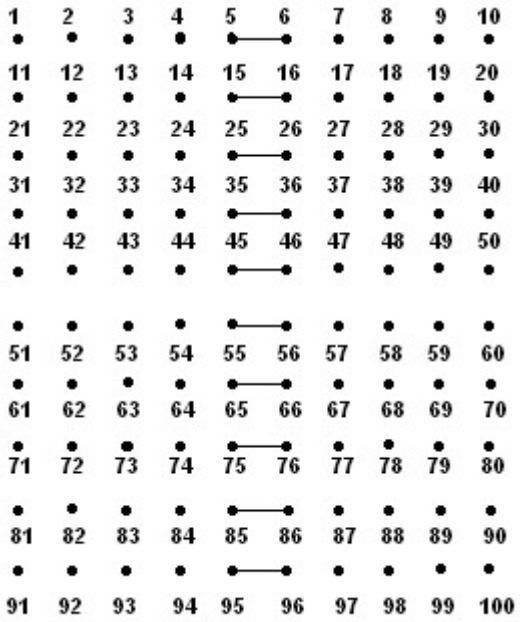


Рис.5.3.Граф ЦЗ (M=100)

При такій математичній моделі зображення стає очевидною область стрибків функції яскравості, найбільш придатна, з урахуванням особливостей людського зору, для вбудови ДІ. Вбудову має сенс здійснювати в ті пікселі контейнера, яким у графі зображення відповідають вузли, ступінь яких не дорівнює нулю, тобто вузли, що не є ізольованими (рис.5.4).

На практиці зручно після залучення чергового пікселя при виконанні вбудови ДІ вузли графа, один з яких відповідає розглянутому пікселю, а другий - суміжний з ним, зробити ізольованими.

а б в

Рис.5.4. Контейнер (а); стеганоповідомлення, сформоване методом випадкового інтервалу (б); стеганоповідомлення з ДІ, що вбудована в область, яка визначається графом (в)

Однієї із проблем, пов'язаних з ЦВЗ, є різноманіття вимог до них, залежно від конкретики їх застосування. Розглянемо докладніше основні області застосування ЦВЗ.

Спочатку розглянемо проблему піратства, або необмеженого неавторизованого копіювання. «Аліса» продає своє мультимедійне повідомлення «Пітеру». Хоча інформація могла бути зашифрована під час передачі, ніщо не перешкодить Пітеру зайнятися її копіюванням після розшифрування. Отже, у цьому випадку потрібен додатковий рівень захисту від копіювання. Існує можливість вбудови ЦВЗ, що дозволяє відтворення й забороняє копіювання інформації.

Важливою проблемою є визначення подліності отриманої інформації, тобто її автентифікація. Зазвичай для автентифікації даних використовуються засоби цифрового підпису, однак ці засоби не зовсім підходять для забезпечення автентифікації мультимедійної інформації. Справа в тому, що повідомлення з електронним цифровим підписом повинно зберігатися й передаватися абсолютно точно, «біт у біт». Мультимедійна ж інформація може незначно спотворюватися як при зберіганні (за рахунок стиску), так і при передачі (вплив одиночних або пакетних помилок у каналі зв'язку). При цьому її якість залишається припустимою для користувача, але цифровий підпис працювати не буде. Одержувач не зможе відрізнити істине, хоча й трохи спотворене повідомлення, від хибного. Крім того, мультимедійні дані можуть бути перетворені з одного формату в інший. При цьому традиційні засоби захисту цілісності працювати також не будуть. Можна сказати, що ЦВЗ здатні захистити саме зміст аудіо-, відеоповідомлення, а не його цифрове представлення у вигляді послідовності біт. Крім того, важливим недоліком цифрового підпису є те, що його легко вилучити із завіреного ним повідомлення, після чого прилаштувати до повідомлення новий підпис. Видалення підпису дозволить порушникові відмовитися від авторства, або ввести в оману законного одержувача щодо авторства повідомлення. Система ЦВЗ проектується таким чином, щоб виключити можливість подібних порушень.

Популярність мультимедіа-технологій викликала безліч досліджень, пов'язаних з розробкою алгоритмів ЦВЗ для використання в стандартах MP3, MPEG-4, JPEG2000, захисту DVD дисків від копіювання.

Питання

1. Вимоги, що висуваються при проектуванні стеганосистеми.
2. Метод модифікації найменшого значущого біта, його переваги, недоліки. Область застосування.
3. Які модифікації методу модифікації найменшого значущого біта можуть застосовуватися? З чим це пов’язано?
4. Як визначається граф цифрового зображення?

5. Що таке припустимий стрибок функції?
6. Як граф зображення застосовується для визначення пікселів, що є найбільш придатними для використання при вбудові додаткової інформації?

Тема 6. ВЛАСТИВОСТІ СТЕГАНОСИСТЕМИ

План

1. Атаки на стеганосистему
2. Надійність сприйняття стеганоповідомлення, її кількісна оцінка
3. Пропускна спроможність каналів передачі інформації, що приховується
4. Стійкість стеганосистеми

1. Атаки на стеганосистему

Стеганосистема утворює стеганоканал, по якому передається СП. Цей канал вважається підданим впливам з боку порушників. У стеганографії зазвичай розглядається така постановка завдання («проблема ув'язнених»). Двоє ув'язнених, Аліса й Боб, бажають конфіденційно обмінюватися повідомленнями, не зважаючи на те, що канал зв'язку між ними контролює охоронець Віллі. Для того, щоб таємний обмін повідомленнями був можливий, передбачається, що Аліса й Боб мають деякий відомий обом секретний ключ. Дії Віллі можуть полягати не тільки в спробі виявлення прихованого каналу зв'язку, але й у руйнуванні переданих повідомлень, а також їх модифікації й створенні нових, хибних повідомлень. Відповідно, можна виділити три типи порушників, яким повинна протистояти стегосистема: *пасивний, активний і злочинний порушники*.

1. *Пасивний порушник* може лише виявити факт наявності стегоканала й (можливо) читати повідомлення. Чи зможе він прочитати повідомлення після його виявлення залежить від стійкості системи шифрування, і це питання, як правило, не розглядається в стеганографії. Якщо в порушника є можливість виявити факт наявності прихованого каналу передачі повідомлень, то стеганосистема зазвичай вважається нестійкою. Хоча існують і інші точки зору на стійкість стегосистем. Здійснення виявлення стеганоканалу є найбільш трудомістким завданням, а захист від виявлення вважається основним завданням стеганографії за визначенням.
2. Діапазон дій *активного* порушника значно ширше. Приховане повідомлення може бути їм вилучене або зруйноване. У цьому випадку адресат, можливо, довідається про факт втручання. У більшості випадків це суперечить інтересам порушника (наприклад, за юридичними мотивами). Інша справа - видалення або руйнування цифрового водяного знака, які можуть розглядатися як основні погрози в цій області.
3. Дії злочинного порушника найнебезпечніші. Він здатний не тільки руйнувати, але й створювати хибні СП. Історія протистояння розвідки й контррозвідки знає чимало прикладів, коли реалізація цієї погрози приводила до катастрофічних наслідків. Ця погроза актуальна й стосовно систем ЦВЗ. Володіючи здатністю створювати водяні знаки, порушник може створювати копії контенту, що захищається, створювати хибні оригінали й т.д.

Для здійснення тієї або іншої погрози порушник застосовує атаки.

Найбільш проста атака - *суб'єктивна*. Порушник уважно розглядає зображення (слухає аудіозапис), намагаючись визначити “на око”, чи є в ньому приховане повідомлення. Ясно, що подібна атака може бути проведена лише проти зовсім незахищених стеганосистем, проте, вона найпоширеніша на практиці, принаймні, на початковому етапі розкриття стеганосистеми.

Суб’єктивна атака, будкчи одною з найпоширеніших стеганографічних атак, не єдина. За аналогією з криптоаналізом у стеганографії можна виділити наступні атаки:

- *Атака на основі відомого заповненого контейнера*. У цьому випадку в порушника є одне або декілька СП. В останньому випадку передбачається, що вбудова приховуваної інформації здійснювалося одним способом. Завдання порушника може полягати у виявленні факту наявності стеганоканалу (основна), а також у його декодуванні або визначенні ключа. Знаючи ключ, порушник одержить можливість аналізу інших стеганоповідомлень.
- *Атака на основі відомого вбудованого повідомлення*. Цей тип атаки більшою мірою характерний для систем захисту інтелектуальної власності, коли в якості водяного знака використовується відомий логотип фірми. Завданням аналізу є отримання ключа. Якщо відповідний до прихованого повідомлення заповнений контейнер невідомий, то завдання розв'язується вкрай важко.
- *Атака на основі обраного прихованого повідомлення*. У цьому випадку порушник має можливість пропонувати для передачі свої повідомлення й аналізувати СП, які виходять.
- *Атака на основі обраного заповненого контейнера*. Цей тип атаки більше характерний для систем ЦВЗ. Стегоаналітик має детектор СП у вигляді «чорного ящика» і декілька СП. Аналізуючи детектовані приховані повідомлення, порушник намагається розкрити ключ.

У порушника може бути можливість застосувати ще три атаки, що не мають прямих аналогій у криптоаналізі:

- *Атака на основі відомого порожнього контейнера*. Якщо він відомий порушникові, то шляхом порівняння його з передбачуваним СП він завжди може встановити факт наявності стеганоканалу. Незважаючи на тривіальність цього випадку, у ряді робіт приводиться його інформаційно-теоретичне обґрунтування. Набагато цікавіше сценарій, коли контейнер відомий приблизно, з деякою похибкою (як це може мати місце при додаванні до нього шуму).
- *Атака на основі обраного порожнього контейнера*. У цьому випадку порушник здатний змусити користуватися запропонованим їм контейнером. Наприклад, запропонований контейнер може мати великі однорідні області (однотонні зображення), і тоді буде важко забезпечити таємність вбудови.
- *Атака на основі відомої математичної моделі контейнера або його частини*. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі. Наприклад, припустимо, що біти усередині зображення коррельовані. Тоді відсутність такої кореляції може служити сигналом про наявне приховане повідомлення. Завдання того, хто вбудовує повідомлення, полягає в тому, щоб не порушити статистики контейнера. Ті, хто вбудовує ДІ, і атакує, можуть мати у своєму розпорядженні різні моделі сигналів, тоді у противоборстві переможе той, хто має кращу модель.

Розглянуті вище атаки мають одну особливість: вони не змінюють стеганоповідомлення. У цьому полягає їхня позитивна сторона: дії порушника навряд чи здатні насторожити відправника й одержувача.

Атаки іншого типу - це *атаки проти вбудованого повідомлення*, які змінюють стеганоповідомлення, а значить можуть змінити й вбудовану в контейнер інформацію. Однією з таких атак є атака, заснована на застосуванні алгоритму стиску Jpeg до СП. Однак набагато більше представлення про переваги того або іншого стеганоалгоритму можна одержати, комплексно використовуючи різні атаки. Загальнодоступна в Інтернеті програма Stirmark дозволяє більш повно аналізувати робастність (стійкість) стегоалгоритмів.

Геометричні атаки - найнебезпечніші на сьогоднішній день, вони змінюють стеганоповідомлення шляхом внесення просторових або часових спотворень, також будучи атаками проти вбудованого повідомлення. Геометричні атаки математично моделюються як аффінні перетворення з невідомим декодеру параметром. Аффінні

перетворення: масштабування, зміна пропорцій, повороти, зсув й усікання. Ці атаки приводять до втрати синхронізації в детекторі ДІ й можуть бути локальними або глобальними (тобто застосованими до всього сигналу). При цьому можливо вирізання окремих пікселів або рядків, перестановка їх місцями, застосування якихось перетворень і т.д. Подібні атаки реалізовані в програмах Unsign (локальні атаки) і Stirmark (локальні й глобальні атаки).

Перераховані стеганографічні атаки не вичерпують усього їх різноманіття, будучи найбільше широко й часто використовуваними.

2.Надійність сприйняття стеганоповідомлення, її кількісна оцінка

Для більшості сучасних методів, які використовуються для приховання повідомлень у файлах цифрового формату при організації прихованого каналу зв'язку, має місце залежність надійності сприйняття СП від обсягу даних, що вбудовуються, представлена на рис.6.1, де очевидним є той факт, що збільшення обсягу даних, що вбудовуються, значно знижує надійність сприйняття СП.

Надійність сприйняття - суб'єктивна характеристика: спотворення контейнера за рахунок вбудови ДІ не повинне бути помітно людині. Таким чином, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги, хоча робота в цьому напрямку ведеться дуже активно, із залученням великого математичного апарата.

Рис.6.1. Взаємозв'язок між надійністю сприйняття стеганоповідомлення й обсягом приховуваного повідомлення при незмінному розмірі контейнера

Нехай у якості контейнера розглядається зображення в градаціях сірого, $n \times n$-матриця якого позначається F. Вбудову ДІ в контейнер, незалежно від способу й області цієї вбудови, можна представити як збурення ΔF поданої матриці F. Матриця стеганоповідомлення $\overline{F}$ очевидно задовольняє співвідношенню:

$$\overline{F} = F + \Delta F \text{, де } \Delta F = f(F), \tag{6.1}$$

тобто ΔF є деякою функцією F.

Будь-які перетворення, які проводяться над СП при його транспортуванні або зберіганні, включаючи активні атакуючі дії, будемо розглядати як додаткові збурення матриці контейнера F.

Дотепер при аналізі рівня візуальних спотворень, які вносяться в контейнер при стегоперетворенні, широко застосовуються різницеві показники, що ґрунтуються на різних модифікаціях відношення «сигнал-шум»:

Різницеві показники рівня візуальних спотворень ЦЗ:

- відношення «сигнал-шум»: $SNR = \frac{\|F\|_F^2}{\|\Delta F\|_F^2}$;
- максимальне (пікове) відношення «сигнал-шум»: $PSNR = \frac{n^2 \max\limits_{i,j} f_{ij}^2}{\|\Delta F\|_F^2}$;
- якість зображення: $IF = 1 - \frac{\|\Delta F\|_F^2}{\|F\|_F^2}$,

де $\|\bullet\|_F$ - матрична норма Фробеніуса ($\|F\|_F = \sqrt{\sum_{i,j=1}^{n} f_{ij}^2}$), хоча слабкі місця таких показників давно відомі (наприклад, відсутність кореляції цих показників із зором людини). Як видне з наведеного на рис.6.2 ілюстративного прикладу, пікове відношення «сигнал-шум» PSNR може бути значним, але при цьому відбувається явне порушення надійності сприйняття (рис.6.2 (б)), а при набагато меншому значенні PSNR видимі зміни на ЦЗ не спостерігаються.

Широке використання різницевих показників спотворення ЦЗ пояснюється тим, що всі існуючі моделі зорового сприйняття є лише частковим і обмеженим відображенням зорової системи людини в силу її складності, а показники спотворення, засновані на таких моделях, інформація про які доступна з відкритих джерел, усе ще залишаються недосконалими й досить складними в реалізації.

а

б

в

Рис.6.2. Ілюстрація недосконалості різницевих показників для оцінки візуальних спотворень ЦЗ: а - вхідне ЦЗ, б - спотворене ЦЗ (*PSNR* = 48 *dB*), в – спотворене за допомогою гауссівського шуму ЦЗ (*PSNR* =28 *dB*)

Оскільки стеганоперетворення контейнера, а також збурні дії, які зазнає стеганоповідомлення, повинні забезпечувати надійність його сприйняття, то $\|\Delta F\|$ не може бути нескінченно великою (де ΔF - матриця збурення контейнера або СП), оскільки у цьому випадку достовірною подією виявиться порушення висунутої вимоги. Крім того, при $\|\Delta F\| \to 0$ імовірність забезпечення надійності сприйняття для СП буде прямувати до одиниці для кожного контейнера. Значення згаданих вище різницевих показників для заданого зображення F визначаються $\|\Delta F\|_F$: чим меньше $\|\Delta F\|_F$, тим краще кількісний показник візуального спотворення F для кожного з них. Враховуючи це, далі будемо вважати, що, чим менше $\|\Delta F\|_F$, тим більше ймовірність забезпечення надійності сприйняття для зображення з матрицею $F + \Delta F$ при заданному вхідному ЦЗ F.

Таким чином, для забезпеченні досить високої ймовірності збереження надійності сприйняття стеганоповідомлення при заданому контейнері стеганометод повинен забезпечувати малу норму (зокрема, Фробеніуса) матриці збурення при стеганоперетворенні.

3. Пропускна спроможність каналів передачі прихованої інформації

Для стеганографічних систем важливо визначити, наскільки великою може бути пропускна спроможність каналів передачі приховуваних повідомлень, і як вона залежить від інших характеристик стеганосистем і умов їх використання. Неформально визначимо, що під *пропускною спроможністю* каналів передачі приховуваних повідомлень або просто пропускною спроможністю прихованого каналу зв'язку (ПСПК) будемо розуміти максимальну кількість інформації, яка може бути вкладене в один елемент контейнера. При цьому приховувані повідомлення повинні бути безпомилково передані одержувачеві й захищені від атак порушника, таких як спроби виявлення факту наявності каналу прихованому зв'язку, читання приховуваних повідомлень, навмисного введення хибних повідомлень або руйнування вбудованої в контейнер інформації. Канал прихованого зв'язку утворюється усередині каналу відкритого зв'язку (каналу загального користування). Пропускна спроможність каналу відкритому зв'язку визначається як кількість інформації, яку потенційно можна передати без помилок за одне використання каналу. При цьому не пред'являється ніяких вимог до захищеності від атак організованого порушника. Тому логічно припустити, що ПСПК повинна бути менше пропускної спроможності каналу відкритого зв'язку, у якому за одне використання каналу передається один елемент контейнера, у який вкладена приховувана інформація.

4.Стійкість стеганосистеми

У порівнянні з достатньо добре дослідженими криптографічними системами, поняття й оцінки безпеки стеганографічних систем більш складні й допускають більше число їх тлумачень. Зокрема, це пояснюється як недостатнім теоретичним і практичним проробленням питання безпеки стеганосистем, так і великою різноманітністю завдань стеганографічного захисту інформації. Стеганосистеми водяних знаків, зокрема, повинні виконувати завдання захисту авторських і майнових прав на електронні повідомлення при різних спробах активного порушника спотворення або стирання вбудованої в них автентифікуючої інформації. Формально говорячи, системи ЦВЗ повинні забезпечити автентифікацію відправників електронних повідомлень. Подібне завдання може бути покладеним на криптографічні системи електронного цифрового підпису (ЕЦП) даних, але на відміну від стеганосистем водяних знаків, відомі системи ЕЦП не забезпечують захист авторства не тільки цифрових, але й аналогових повідомлень, і в умовах, коли активний порушник вносить спотворення в повідомлення, що захищається, й автентифікуючу інформацію. Інші вимоги по безпеці пред'являються до стеганосистем, призначеним для приховання факту передачі конфіденційних повідомлень від пасивного порушника.

Як і для криптографічних систем захисту інформації, безпека стеганосистем описується й оцінюється їхньою стійкістю (стеганографічною стійкістю або для стислості стеганостійкістю*).* ***Під стійкістю різних стеганосистем розуміється їхня здатність приховувати від кваліфікованого порушника факт прихованої передачі повідомлень, здатність протистояти спробам порушника зруйнувати, спотворити, вилучити потай передані повідомлення, а також здатність підтвердити або спростувати автентичність потай переданої інформації****.*

Дослідимо стегосистеми, завданням яких є прихована передача інформації. У криптографічних системах ховається зміст конфіденційного повідомлення від порушника, у той час як у стеганографії додатково ховається факт існування такого повідомлення. Тому визначення стійкості й злому цих систем різні. У криптографії система захисту інформації є стійкою, якщо, маючи перехоплену криптограму, порушник не здатний читати повідомлення, що міститься в ній. Неформально визначимо, що *стеганосистема є стійкою, якщо порушник, спостерігаючи інформаційний обмін між відправником і одержувачем, не здатний виявити, що під прикриттям контейнерів передаються приховувані повідомлення, і тим більше читати ці повідомлення*.

Назвемо в загальному випадку стеганосистему нестійкою, якщо протиборча сторона здатна виявляти факт її використання. Розглянемо спрощену базову модель стеганосистеми (рис.6.3), у якій у кодері використовується стеганографічна функція f вбудови по секретному ключу K повідомлення M, що приховується, в контейнер C, а в декодері стеганографічна функція φ його витягу по тому ж ключу. Із СП по функції φ витягається вбудоване повідомлення $\hat{I}$ і при необхідності контейнер $\hat{N}$.

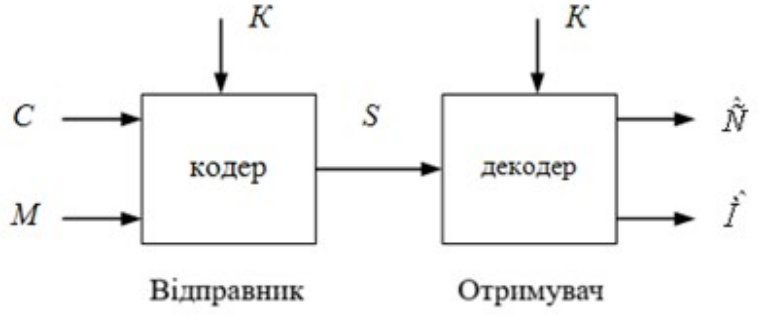


Рис. 6.3. Базова модель стегосистеми

У результаті спотворень при вбудовуванні, впливу випадкових і навмисних перешкод передачі, а також похибок при витягу відновлене одержувачем повідомлення $\hat{I}$ може відрізнятися від оригіналу *M*. Аналогічно, отриманий контейнер $\hat{N}$ буде відрізнятися від поданого *C*. Контейнер буде спотворюватися при вбудовуванні приховуваного повідомлення. У ряді стеганосистем необхідно відновлювати контейнер, тому що він фізично являє собою звичайні повідомлення (зображення, мовні сигнали) кореспондентів відкритого зв'язку, під прикриттям яких здійснюється прихований зв'язок. Ці повідомлення відкритого зв'язку повинні доставлятися їхнім одержувачам з якістю, обумовленою встановленими вимогами до вірогідності відкритого зв'язку. Однак навіть якщо використовуваний контейнер є тільки переносником приховуваного повідомлення, ступінь припустимої погрішності контейнера також повинна бути обмеженою, тому що інакше порушник легко виявить факт використання стеганосистеми.

Очевидно, що стійкість стеганосистеми повинна забезпечуватися при використанні несекретних (загальновідомих) функцій вбудовування f і витягу φ. Безпека стеганосистем (за принципом Керхгоффа) повинна опиратися на такі принципи їх побудови, при яких якщо порушник не знає секретної ключової інформації, то навіть при повному знанні функцій вбудовування й витягу приховуваної інформації, законів розподілу приховуваних повідомлень, контейнерів і СП він не здатний установити факт прихованої передачі інформації.

Стійкість різних стеганосистем може бути розділена на:

1. Стійкість до виявлення факту передачі (існування) приховуваної інформації,
2. Стійкість до витягу приховуваної інформації,
3. Стійкість до нав'язування хибних повідомлень по каналу прихованого зв'язку (імітостійкість),
4. Стійкість до відновлення секретного ключа стегосистеми,
5. Стійкість до атак проти вбудованого повідомлення.

Очевидно, що якщо стеганосистема є стійкою до виявлення факту передачі (існування) приховуваної інформації, то логічно припустити, що вона при цьому є стійкою й до читання приховуваної інформації. Зворотне в загальному випадку невірно. Стеганосистема може бути стійкою до читання приховуваної інформації, але факт передачі інформації під прикриттям контейнера може виявлятися порушником.

Стійкість стеганосистеми до нав'язування хибних повідомлень по каналу прихованого зв'язку характеризує її здатність виявляти й відкидати сформовані порушником повідомлення, що вводяться їм у канал передачі приховуваних повідомлень із метою видачі їх за оригінальні, такі, що виходять від законного відправника. Якщо в системі ДІ зловмисник здатний увести в контейнер, завірений законним відправником, свій водяний знак, і детектор буде виявляти водяний знак зловмисника й не виявляти ЦВЗ дійсного відправника, то це означає дискредитацію (злом) системи ЦВЗ.

Стійкість до відновлення секретного ключа стеганосистеми характеризує її здатність протистояти спробам порушника обчислити секретну ключову інформацію даної стеганосистеми. Якщо порушник здатний визначити ключ стеганосистеми, то він може однозначно виявляти факти передачі приховуваних повідомлень і читати їх або нав'язувати хибні повідомлення без усяких обмежень. Таку подію можна назвати повною компрометацією стеганосистеми. Очевидно, що атаки порушника на ключ стеганосистеми можуть бути побудовані аналогічно атакам на ключ систем шифрування інформації й систем автентифікації повідомлень.

Якщо порушник здатний обчислити ключ вбудовування водяного знака якого-небудь автора (власника) інформаційних ресурсів, то він може поставити цей водяний знак на будь-який контейнер. Тим самим порушник дискредитує або водяний знак даного автора (власника), або цілком усю систему ЦВЗ. В обох випадках ставиться під сумнів законність прав одного або всіх власників інформаційних ресурсів на те, що дійсно їм належить.

Дана проблема має велике практичне значення для захисту авторських і майнових прав виробників різного роду інформаційних продуктів, таких як ліцензійне програмне забезпечення, CD і DVD дисків, відео й аудио касет і т.п. Світовий ринок інформаційної індустрії оцінюється багатьма мільярдами доларів у рік і тому не дивно, що захист інформації як товару, від різних зазіхань зловмисників швидко здобуває конкретну практичну спрямованість.

Стійкість стеганосистеми до атак проти вбудованого повідомлення вже обговорювалася вище.

Питання

1. Визначення пасивного, активного і злочинного порушника.
2. Суб'єктивна атака на стеганосистему.
3. Атаки на стеганосистему за аналогією з крипто аналізом.
4. Специфічні атаки на стеганосистему.
5. Атаки проти вбудованого повідомлення.
6. Геометричні атаки.
7. Надійність сприйняття стеганоповідомлення, її кількісна оцінка.
8. Різницеві показники рівня візуальних спотворень ЦЗ.
9. Пропускна спроможність каналів передачі прихованої інформації.
10. Що розуміється під стійкістю стеганосистеми?
11. Як визначається:
    - стійкість до виявлення факту передачі (існування) приховуваної інформації,
    - стійкість до витягу приховуваної інформації,
    - стійкість до нав'язування хибних повідомлень по каналу прихованого зв'язку,
    - стійкість до відновлення секретного ключа стегосистеми,
    - стійкість до атак проти вбудованого повідомлення?

Тема 7. СТЕГАНОПЕРЕТВОРЕННЯ В ЧАСТОТНІЙ ОБЛАСТІ КОНТЕЙНЕРА. МЕТОД КОХА І ЖАО

План

1. Особливості й переваги використання частотної області контейнера для стеганоперетворення
2. Метод Коха і Жао

1. Особливості й переваги використання частотної області контейнера для стеганоперетворення

Забезпечення стійкості стеганографічного методу до різних атак - задача актуальна й нетривіальна. Складність забезпечення цієї стійкості залежить від того, яка область контейнера (просторова, частотна, іншого перетворення) використовується для вбудови ДІ. Забезпечити стійкість до атак проти вбудованого повідомлення в просторовій області ЦЗ-контейнера складніше, чим у частотній, хоча це жодним чином не означає, що неможливо забезпечити нечутливість стеганоповідомлення в просторовій області.

Існує кілька способів представлення ЦЗ у частотній області. При цьому використовується ця чи інша декомпозиція ЦЗ-контейнера. Наприклад, існують методи на основі використання дискретного косинусного перетворення, дискретного

перетворення Фурьє, вейвлет-перетворення та ін. Такі перетворення можуть застосовуватися чи до окремих частин ЦЗ, чи до зображення в цілому. Найбільше поширення серед таких перетворень в стеганографії отримали вейвлет-перетворення і ДКП, що певною мірою пояснюється їх застосуванням в алгоритмах стиску ЦЗ. Крім того, застосування при приховуванні данних саме того перетворення зображення, якому це зображення буде піддаватися під час можливої атаки, є доцільним, оскільки в такому випадку можливо врахувати всі особливості перетворення для підвищення ймовірності збереження ДІ. Наприклад, враховуючи, що алгоритм ДКП є базою в стандарті Jpeg, а вейвлет-перетворення – в Jpeg2000, доцільно при вбудові ДІ, якщо передбачається стиск ЦЗ-стеганоповідомлення алгоритмом Jpeg, використовувати область ДКП, а якщо стеганоповідомлення може піддатися атаці стиском з використанням Jpeg2000, то вбудову ДІ проводити саме в області дискретного вейвлет-перетворення. Зауважимо, що таке врахування специфікі можливих атак на стеганоповідомлення є доцільним, є найбільш простим, але це не означає, що обовязковим, тобто, наприклад, забезпечення стійкості стеганоалгоритму до стиску Jpeg може бути проведеним не тільки тоді, коли вбудова ДІ відбувається в області ДКП. Існує первна кількість стеганоалгоритмів, які проводять вбудову ДІ в просторовій області контейнера, в області сингулярного (спектрального) розкладання, але є стійкими до атак проти вбудованого повідомлення, зокрема до атаки стиском.

Відомо, що реальні ЦЗ не представляють собою випадкові процеси, більша частина енергії ЦЗ сконцентрована в низькочастотній складовій. Високочастотні складові ЦЗ найбільшим чином піддаються впливу з боку різноманітних алгоритмів обробки зображення, таких як стиск, низько-частотна фільтрація тощо. Таким чином, можна зробити висновок, що для вбудови ДІ найбільш прийнятною є середньо-частотна складова його спектру.

2. Метод Коха і Жао

Розглянемо один зі стеганографічних методів, який позиціонується, як стійкий до незначних атак проти вбудованого повідомлення: метод відносної заміни величин коефіцієнтів дискретного косинусного перетворення (метод Коха й Жао) - це один з найпоширеніших на сьогодні методів прихування конфіденційної інформації в частотній області зображення, який полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП).

На початковому етапі первинне зображення стандартним чином розбивається на $8\times 8-$блоки. До кожного блоку, який будемо позначати B, застосовується ДКП, тим самим здійснюючи переведення кожного блоку із просторової в частотну область. У результаті виходить $8\times 8-$блок коефіцієнтів ДКП. Кожний блок призначено для прихування одного біта ДІ.

Існує дві реалізації алгоритму:

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

Розглянемо докладно перший варіант.

Під час організації прихованого каналу зв'язку абоненти повинні попередньо домовитися (зв'язатися по захищеному каналу зв'язку) про два конкретних коефіцієнта ДКП із кожного блоку, які будуть використовуватися для прихування даних. Задамо дані коефіцієнти їх індексами (u_1, v_1) і (u_2, v_2) в масивах коефіцієнтів ДКП:

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

Відмітимо, що зазначені індекси повинні відповідати середньочастотним коефіцієнтам ДКП, що забезпечить:

- Прихованість інформації;
- Вбудована інформація не буде спотворюватися при Jpeg-стиску зі значними коефіцієнтами якості (або, що те ж саме, з малими коефіцієнтами стиску).

На практиці найчастіше використовуються $(u_1,v_1)=(4,5)$ і $(u_2,v_2)=(5,4)$.

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

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

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

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

Таким чином, первинне зображення спотворюється за рахунок внесення змін у коефіцієнти ДКП, якщо їх відносні величини не відповідають приховуваному біту. Чим більше P, тем стеганосистема, створена на основі даного методу, є більш стійкою до стиску, однак якість зображення при цьому може значно погіршитися (рис.7.1).

а

б

в

Рис. 7.1. Приклад використання алгоритму Коха й Жао: а - оригінальне ЦЗ-контейнер; б - стеганоповідомлення, отримане з використанням P=25; в - стеганоповідомлення, отримане з використанням P=75

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

У результаті пересилання стеганоповідомлення, як уже говорилося вище, зазнає спотворення, спотворення зазнає й ДІ.

Для витягу ДІ виконується аналогічна процедура вибору коефіцієнтів ДКП у кожному блоці, що були задіяні в теганоперетвореннi, а розв'язок про переданий біт ухвалюється у відповідності з наступним правилом:

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

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

Питання

1. Як відбувається стеганоперетворення в частотній області цифрового зображення?
2. Чому частотна область вважається кращою для стеганоперетворення, стійкого до атак проти вбудованого повідомлення?
3. Де відбувається вбудова ДІ у методі Коха та Жао?
4. Скільки та які коефіцієнти ДКП задіяні у стеганоперетвореннi у методі Коха та Жао? Чому?
5. Як відбувається декодування у методі Коха та Жао?

Тема 8. СТЕГАНОГРАФІЧНИЙ МЕТОД, ЩО ЗАБЕЗПЕЧУЄ ВИСОКУ ПРОПУСКНУ СПРОМОЖНІСТЬ ПРИХОВАНОГО КАНАЛУ ЗВ'ЯЗКУ

План

1. Стеганометод, заснований на нормальному сингулярному розкладанні матриці
2. Алгоритмічна реалізація стеганометоду, заснованому на нормальному сингулярному розкладанні матриці
3. Симетрична реалізація методу.

1. Стеганометод, заснований на нормальному сингулярному розкладанні матриці

Нехай

$$p_1, p_2, ..., p_l \qquad (8.1)$$

- результат попереднього кодування конфіденційної інформації, при цьому $p_i \in \{-1,1\}$. Такий результат може бути отриманий з бінарної послідовності звичного виду, коли її елементи належать $\{0,1\}$, шляхом ще одного кроку в попередньому кодері:

$$\begin{matrix} 0 \to -1 \\ 1 \to 1 \end{matrix}.$$

Опис алгоритму проводиться для ЦЗ-контейнера в градаціях сірого, однак алгоритм може бути застосований і до кольорового ЦЗ - до кожної колірної складової окремо.

Матриця ЦЗ-контейнер розбивається стандартним чином на $n \times n-$блоки. Якщо число рядків/стовпців у матриці зображення не кратне *n*, то рядки/стовпці, що залишилися після розбивки, не беруть участь у процесі стеганоперетворення (ігноруються).

Нехай A – довільний $n \times n-$блок ЦЗ-контейнера, що використовується в стеганоперетворенні (СПр). Біти ДІ вбудовуються у блок А з використанням наступного чотирикрокового процесу.

Крок 1. Для A обчислити нормальне сингулярне розкладання:

$$A = U\Sigma V^T.$$

Крок 2. Перетворити матрицю U лівих сингулярних векторів в матрицю U' по наступному правилу:

$$u_{ij}' = p_k \left| u_{ij} \right|, \qquad (8.2)$$

де p_k - черговий елемент (8.1), u_{ij} - черговий елемент матриці U, вибір місця розташування якого обґрунтовується нижче, u_{ij}' - результат зміни u_{ij} в процесі СПр, після чого привести інші елементи матриці U до виду, що забезпечує ортогональність її стовпців.

Крок 3. Обчислити:

$$A' = U'\Sigma V^T.$$

Крок 4. Забезпечити, щоб значення елементів A' належали множині $\{0,1,...,255\}$. Результат: $\overline{A}$ - блок ЦЗ-стеганоповідомлення.

Декодування вбудованої ДІ виконується у відповідності з наступними кроками. Нехай $\overline{A}$ - черговий блок СП, у який вбудовувалася ДІ.

Крок 1. Побудувати нормальне сингулярне розкладання $\overline{A}$:

$$\overline{A} = \overline{U}\,\overline{\Sigma}\,\overline{V}^T .$$

Крок 2. Декодування чергових елементів ДІ провести з відповідних елементів матриці $\overline{U}$ відповідно до формули:

$$p_k = \frac{\overline{u}_{ij}}{\left|\overline{u}_{ij}\right|}, \quad j = 3,...,7, \quad i = 2,...,9-j .$$

2.Алгоритмічна реалізація стеганометоду, заснованому на нормальному сингулярному розкладанні матриці

Розглянемо докладно крок 2. Надійність сприйняття стеганоповідомлення (СП) повинна зберігатися обов'язково, а її порушення є дуже ймовірним, якщо зміні в процесі СПр будуть піддаватися елементи першої сингулярної тройки (тройка, що відповідає максимальному СНЧ) (див. Лекція 3). Тому в даному алгоритмі СНВ, що відповідають максимальному СНЧ, при СПр не задіюються. Взагалі кількість таких стовпців в U, V (таких СНВ) є параметром алгоритма, який можна змінювати. Нехай m - це число перших стовпців в U, які залишаються незмінними.

Далі покладається $n = 8$, $m = 2$, тобто в процесі СПр будуть змінюватися 6 правих стовпців матриці U кожного $8\times 8-$блока, що задіюється в СПр. В кожний блок буде вбудовуватися 15 біт ДІ. Схематично області матриці U представлені на рис. 8.1.

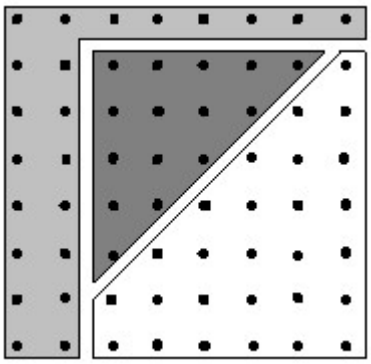


Рис.8.1. Матриця U : світло-сіра область не задіюється в СПр, темно-сіра область змінюється відповідно до крока 2 алгоритму, біла область перетворюється для забезпечення ортогональності стовпців матриці U після СПр

Відмітимо, що якщо два перші стовпці U не задіяні в процесі СПр для того, щоб не викликати порушень надійності сприйняття стеганоповідомлення, то перший рядок залишається незмінним в силу того, що він забезпечує лексикографічну додатність стовпців U (і відповідно єдиність сингулярного розкладання A). Біти ДІ вбудовуються відповідно до формули (8.2), яка може бути уточнена відповідно до розглянутих параметрів ($n = 8$, $m = 2$):

$$u_{ij}' = p_k\left|u_{ij}\right|, \quad j = 3,...,7, \quad i = 2,...,9-j . \qquad (8.3)$$

В результаті (8.3) елементи матриці U' з індексами $j=3,...,7,\quad i=2,...,9-j$ можуть відрізнятися від відповідних елементів матриці U тільки знаком. Знак елемента $u_{ij}',\quad j=3,...,7,\quad i=2,...,9-j$ матриці U' - це і є вбудований біт ДІ.

Тепер необхідно використовувати елементи з білої області матриці U (рис.8.1), щоб забезпечити ортогональність матриці U'. Нехай

U'_i - позначення для *i*-ого стовпця U'.

Ортогональність U' означає, що

$$\left(U'_i,U'_j\right)=\delta_{ij}=\begin{cases}1, & i=j,\\ 0, & i\neq j.\end{cases}, \tag{8.4}$$

де $\left(U'_i,U'_j\right)$ - скалярний добуток векторів U'_i,U'_j.

Стовпці U'_1 і U'_2 у матриці U' відомі, вони співпадають з відповідними стовпцями в матриці U. Для стовпця U'_3: $u_{13}'=u_{13}$, елементи $u_{23}',u_{33}',u_{43}',u_{53}',u_{63}'$ визначаються відповідно до (8.3), а от u_{73}',u_{83}' необхідно визначити так, щоб

$$\begin{cases}\left(U'_3,U'_1\right)=0,\\ \left(U'_3,U'_2\right)=0\end{cases}$$

$$\left(U'_3,U'_1\right)=\underbrace{u_{13}'\cdot u_{11}'+u_{23}'\cdot u_{21}'+u_{33}'\cdot u_{31}'+u_{43}'\cdot u_{41}'+u_{53}'\cdot u_{51}'+u_{63}'\cdot u_{61}'}_{\text{відомі}}+u_{73}'\cdot\underbrace{u_{71}'}_{\text{відомий}}+u_{83}'\cdot\underbrace{u_{81}'}_{\text{відомий}}=0$$

$$\left(U'_3,U'_2\right)=\underbrace{u_{13}'\cdot u_{12}'+u_{23}'\cdot u_{22}'+u_{33}'\cdot u_{32}'+u_{43}'\cdot u_{42}'+u_{53}'\cdot u_{52}'+u_{63}'\cdot u_{62}'}_{\text{відомі}}+u_{73}'\cdot\underbrace{u_{72}'}_{\text{відомий}}+u_{83}'\cdot\underbrace{u_{82}'}_{\text{відомий}}=0$$

Одержали систему 2-х лінійних рівнянь із двома невідомими: u_{73}',u_{83}'. Вирішуючи її, знаходимо u_{73}',u_{83}'. Стовпець U'_3 визначений повністю. Переходимо до стовпця U'_4.

Для стовпця U'_4: $u_{14}'=u_{14}$, елементи $u_{24}',u_{34}',u_{44}',u_{54}'$ визначаються відповідно до (8.3), а u_{64}',u_{74}',u_{84}' необхідно визначити так, щоб

$$\begin{cases}\left(U'_4,U'_1\right)=0,\\ \left(U'_4,U'_2\right)=0,\\ \left(U'_4,U'_3\right)=0.\end{cases}$$

$$\left(U'_4,U'_1\right)=\underbrace{u_{14}'\cdot u_{11}'+u_{24}'\cdot u_{21}'+u_{34}'\cdot u_{31}'+u_{44}'\cdot u_{41}'+u_{54}'\cdot u_{51}'}_{\text{відомі}}+u_{64}'\cdot\underbrace{u_{61}'}_{\text{відомий}}+u_{74}'\cdot\underbrace{u_{71}'}_{\text{відомий}}+u_{84}'\cdot\underbrace{u_{81}'}_{\text{відомий}}=0$$

$$\left(U'_4,U'_2\right)=\underbrace{u_{14}'\cdot u_{12}'+u_{24}'\cdot u_{22}'+u_{34}'\cdot u_{32}'+u_{44}'\cdot u_{42}'+u_{54}'\cdot u_{52}'}_{\text{відомі}}+u_{64}'\cdot\underbrace{u_{62}'}_{\text{відомий}}+u_{74}'\cdot\underbrace{u_{72}'}_{\text{відомий}}+u_{84}'\cdot\underbrace{u_{82}'}_{\text{відомий}}=0$$

$$\left(U'_4,U'_3\right)=\underbrace{u_{14}'\cdot u_{13}'+u_{24}'\cdot u_{23}'+u_{34}'\cdot u_{33}'+u_{44}'\cdot u_{43}'+u_{54}'\cdot u_{53}'}_{\text{відомі}}+u_{64}'\cdot\underbrace{u_{63}'}_{\text{відомий}}+u_{74}'\cdot\underbrace{u_{73}'}_{\text{відомий}}+u_{84}'\cdot\underbrace{u_{83}'}_{\text{відомий}}=0$$

Одержали систему 3-х лінійних рівнянь із трьома невідомими: $u_{64}', u_{74}', u_{84}'$. Розвязуючи її, визначаємо $u_{64}', u_{74}', u_{84}'$. Стовпець U'_4 визначений повністю.

Продовжуючи цей процес, визначимо стовпці U'_5, U'_6, U'_7, U'_8. Після цього кожний з отриманих стовпців нормується, тобто ділиться на його довжину (евклидову норму):

$$U'_i = \frac{U'_i}{\|U'_i\|}, \quad i = 3,4,...,8.$$

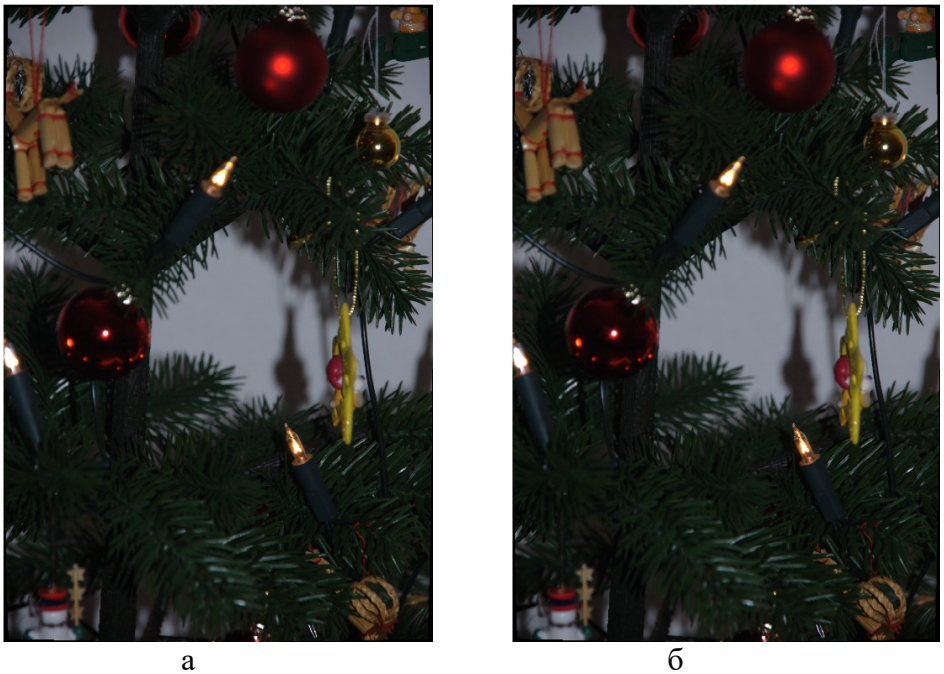
У результаті сформована в такий спосіб матриця U' є ортогональною, а її стовпці – лексикографічно додатними.

На кроці 3 сформована матриця U' множиться на незмінені матриці Σ і V^T, в результаті чого виходить матриця A'. Матриця A' має єдине нормальне сингулярне розкладання: $A' = U'\Sigma V^T$, побудувавши яке, можна витягти 15 біт ДІ з відповідних елементів U'. Але A' ще не можна розглядати як блок ЦЗ-стеганоповідомлення. По-перше, елементи $A' = U'\Sigma V^T$ у загальному випадку є нецілими числами, а по-друге, вони можуть виходити за межі $[0,255]$. Тому матриця A' потребує додаткової обробки, яка відбувається на кроці 4 і полягає в наступному. Результат обробки – блок $\overline{A}$ стеганоповідомлення з елементами $\overline{a}_{ij}$, $i, j = 1,2,...,8$:

$$\overline{a}_{ij} = \begin{cases} [a_{ij}'], \text{ якщо } 0 \le a_{ij}' \le 255, \\ 0, \text{ якщо } a_{ij}' < 0, \\ 255, \text{ якщо } a_{ij}' > 0, \end{cases},$$

де a_{ij}', $i, j = 1,2,...,8$, - елементи матриці A', $[a_{ij}']$ - результат округлення a_{ij}' до найближчого цілого числа.

Запропонована стратегія приводить до стеганоповідомлення, для якого зберігається надійність сприйняття. Ілюстрацією цьому є рис.8.2.



а б

Рис.8.2. Збереження надійності сприйняття СП: а - ЦЗ-контейнер; б - ЦЗ-СП

3.Симетрична реалізація методу

Розглянемо можливість модифікації розглянутого стеганографічного методу з метою ще більшого збільшення пропускної спроможності формованого прихованого каналу зв'язку.

Нехай A - один з отриманих шляхом стандартної розбивки матриці ЦЗ-контейнера $8\times 8-$блоків. Блоку A поставимо у відповідність симетричні блоки B, C по правилу:

$$A=\begin{pmatrix} a_{11}\ a_{12}\ a_{13}...a_{18} \\ a_{21}\ a_{22}\ a_{23}...a_{28} \\ a_{31}\ a_{32}\ a_{33}...a_{38} \\ ..... \\ a_{81}\ a_{82}\ a_{83}...a_{88} \end{pmatrix} \to B=\begin{pmatrix} a_{11}\ a_{12}\ a_{13}...a_{18} \\ a_{12}\ a_{22}\ a_{23}...a_{28} \\ a_{13}\ a_{23}\ a_{33}...a_{38} \\ ..... \\ a_{18}\ a_{28}\ a_{38}...a_{88} \end{pmatrix}, \quad C=\begin{pmatrix} a_{11}\ a_{21}\ a_{31}...a_{81} \\ a_{21}\ a_{22}\ a_{32}...a_{82} \\ a_{31}\ a_{32}\ a_{33}...a_{83} \\ ..... \\ a_{81}\ a_{82}\ a_{83}...a_{88} \end{pmatrix}, \qquad (8.5)$$

нормальні спектральні розкладання яких:

$$B=U_B\Lambda_B U_B^T,\ C=U_C\Lambda_C U_C^T,$$

де стовпці матриць власних векторів U_B і U_C - лексикографічно додатні, тобто перший ненульовий компонент вектора-стовпця є додатним.

Вбудова ДІ пропонованим нижче алгоритмом, що називається SR-алгоритмом, проводиться в стовпці матриць U_B і U_C, вибір яких аналогічний тому, як це робилося вище для лівих сингулярних векторів. Для конкретизації будемо розглядати далі матрицю B. Будемо вважати, що на рис.8.1 схематично представлена матриця власних векторів U_B, вбудова в яку ДІ SR-алгоритмом відбувається у виділену трикутну область відповідно до формули:

$$u_{ij}^{'}=p_k\left|u_{ij}^{(B)}\right|,\ j=\overline{3,7},\ i=\overline{2,9-j},$$

де $u_{ij}^{(B)}$, $u_{ij}^{'}$ — елементи матриці U_B і U' — нових збурених власних векторів відповідно.

Нормування стовпців U' після вбудови ДІ відбувається за рахунок модифікації елементів, що містяться в трапецієподібній області U_B (рис.8.1), шляхом розв'язку неоднорідних СЛАР, з наступною нормалізацією, як це робилося для стеганоалгоритма, заснованого на сингулярному розкладанні, який розглядався вище.

Після вбудови 15 біт ДІ в блок B, обчислюється матриця $B'=U'\Lambda_B U'^T$, елементи якої, загалом кажучи, можуть і не належати множині $\{0,1,...,255\}$. З B' отримуємо матрицю $\overline{\overline{B}}$ тієї ж розмірності наступним стандартним чином: якщо $b_{ij}^{'}<0$, то $\overline{\overline{b}}_{ij}=0$; якщо $b_{ij}^{'}>255$, то $\overline{\overline{b}}_{ij}=255$; якщо $0\le b_{ij}^{'}\le 255$, але не є цілим числом, то $\overline{\overline{b}}_{ij}$ є результатом округлення $b_{ij}^{'}$ до найближчого цілого. Аналогічні операції проробляємо для блоку C, результатом чого є матриця $\overline{\overline{C}}$. Блок $\overline{\overline{A}}$ СП буде мати вид:

$$\overline{\overline{A}} = \begin{pmatrix} a_{11} & \overline{\overline{b}}_{12} & \overline{\overline{b}}_{13} & \dots & \overline{\overline{b}}_{17} & \overline{\overline{b}}_{18} \\ \overline{\overline{c}}_{21} & a_{22} & \overline{\overline{b}}_{23} & \dots & \overline{\overline{b}}_{27} & \overline{\overline{b}}_{28} \\ \overline{\overline{c}}_{31} & \overline{\overline{c}}_{32} & a_{33} & \dots & \overline{\overline{b}}_{37} & \overline{\overline{b}}_{38} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \overline{\overline{c}}_{81} & \overline{\overline{c}}_{82} & \overline{\overline{c}}_{83} & \dots & \overline{\overline{c}}_{87} & a_{88} \end{pmatrix},$$

де $\overline{\overline{b}}_{ij}, \overline{\overline{c}}_{ij}$ — елементи матриць $\overline{\overline{B}}, \overline{\overline{C}}$ відповідно.

Для декодування ДІ по матриці $\overline{\overline{A}}$ отримуємо $\overline{\overline{\overline{B}}}, \overline{\overline{\overline{C}}}$ відповідно до (8.5). Спектральне розкладання матриці $\overline{\overline{\overline{B}}} = \overline{\overline{U}}_B \overline{\overline{\Lambda}}_B \overline{\overline{U}}_B^T$ використовується для відновлення елементів ДІ відповідно до формули: $p_k = \overline{\overline{u}}_{ij}^{(B)} / \left| \overline{\overline{u}}_{ij}^{(B)} \right|, j = \overline{3,8},\ i = \overline{2,9-j}$. Аналогічні операції проводяться з матрицею $\overline{\overline{\overline{C}}}$. Відмітимо, що порядок вбудови елементів секретного повідомлення в блоки B, C може бути частиною секретного ключа.

Для побудованого SR-алгоритму кожний з блоків A контейнера використовується для пересилання 30 біт ДІ (що в 2 рази більше, чим в алгоритмі, розглянутому вище).

Питання

1. Чому в запропонованому стеганометоді використовується нормальне сингулярне розкладання матриці блоку ЦЗ-контейнера, а не звичайне?
2. В чому переваги блокових стеганографічних методів?
3. Чому результатом роботи кодеру при використанні запропонованого стеганографічного методу є бінарна послідовність не в алфавіті {0, 1}, як зазвичай, а в алфавіті {-1, 1}?
4. Якою є пропускна спроможність прихованого каналу в запропонованому стеганографічному методі?
5. Як забезпечується попарна ортонормальність сингулярних векторів блоку після вбудови додаткової інформації?
6. Симетрична реалізація методу. Пропускна спроможність прихованого каналу в симетричній реалізації методу.
7. Переваги та недоліки симетричної реалізації методу.

Тема 9. СТЕГАНОПЕРЕТВОРЕННЯ, СТІЙКЕ ДО АТАКИ СТИСКОМ

План

1. Стеганоперетворення як збурення набору математичних параметрів, що визначають контейнер
2. Особливості СНЧ блоків матриці ЦЗ при стиску з втратами
3. Стеганографічний метод, стійкий до атаки стиском

1. Стеганоперетворення як збурення набору математичних параметрів, що визначають контейнер

У якості формального представлення контейнера, не обмежуючи спільності міркувань, розглядається матриця F.

Перетворення контейнера за рахунок вбудови в нього ДІ, незалежно від способу й області цієї вбудови, можна представити відповідно до формули

$$\overline{F} = F + \Delta F \tag{9.1}$$

як збурення $\Delta F = f(F)$ матриці F, розглядаючи $\overline{F}$ як матрицю стеганоповідомлення.

З формули (9.1) випливає істинність наступного твердження.

***Твердження* 1.** Довільне стеганоперетворення можна представити еквівалентним образом у вигляді адитивної вбудови деякої інформації в просторовій області.

Будь-які перетворення, які проводяться над стеганоповідомленням, будемо розглядати як додаткові збурення матриці контейнера F.

У якості набору параметрів, що однозначно визначають й всебічно характеризують будь-яке ЦЗ, можна використовувати кожний з наборів, який однозначно визначає довільну двовимірну матрицю. Назвемо такі набори параметрів *повними*.

Розглянемо один з можливих повних наборів параметрів.

Нехай F — матриця розміром $m \times n$ з елементами f_{ij}, $i = \overline{1,m}$, $j = \overline{1,n}$, ($m \geq n$).СНЧ і СНВ, одержувані нормальним сингулярним розкладанням матриці, однозначно визначають матрицю, а значить можуть розглядатися як повний набір параметрів для ЦЗ. Далі, говорячи про СНВ, будемо припускати, що вони ортонормовані лексикографічно додатні, тобто однозначно визначаються нормальним сингулярним розкладанням.

Будь-яке перетворення ЦЗ, у тому числі стеганоперетворення, збурить його матрицю F, а тому певним чином збурить його СНЧ і СНВ. У силу цього має місце наступне твердження.

***Твердження* 2.** Стеганоперетворення ЦЗ, результат атак проти вбудованого повідомлення можна формально представити у вигляді сукупності збурень СНЧ і (або) СНВ його матриці, які відбулися в результаті вбудови ДІ, що дозволяє природно звести задачу аналізу процесу стеганоперетворення до аналізу збурень СНЧ і СНВ.

2. Особливості СНЧ блоків матриці ЦЗ при стиску з втратами

Проблема створення стеганографічних алгоритмів (СА), стійких до атаки стиском, яка є надзвичайно розповсюдженою завдяки популярності використання форматів із втратами для зберігання й передачі цифрових сигналів, є актуальною. Найчастіше існуючі СА такого плану здійснюють вбудову секретної інформації в частотній області контейнера й, за умови забезпечення надійності сприйняття стеганоповідомлення, витримують лише незначний стиск, хоча використання на практиці атак стиском з великими коефіцієнтами є подією з великою ймовірністю.

У якості формату із втратами далі для визначеності розглядається Jpeg.

Нехай F - $n \times n$-матриця контейнера. Загальна схема стиску (із втратами) складається із трьох основних кроків: відображення в частотну область після попередньої розбивки матриці зображення на 8×8 – блоки, квантування отриманих коефіцієнтів, ентропійне кодування. Позначимо B матрицю окремого блоку, ΔB - матрицю збурення блока. Для кожного блоку можлива побудова єдиного нормального сингулярного розкладання: $B = U \Sigma V^T$, де U, V — ортогональні матриці розміру 8×8, стовпці $u_1,...,u_8$ матриці U - ліві СНВ, лексикографічно додатні (стовпці $v_1,...,v_8$ матриці V - праві СНВ матриці B); $\Sigma = diag(\sigma_1,...,\sigma_8)$, $\sigma_1 \geq ... \geq \sigma_8 \geq 0$ - СНЧ, збурення яких і будуть аналізуватися в процесі стиску, стеганоперетворення й т.і.

Процес стиску ЦЗ певним чином збурить СНЧ матриць блоків.

Зауваження. Можна показати, що сукупності СНЧ матриць ЦЗ в просторовій і частотній областях співпадають, будь-які збурення СНЧ виявляться однаково для матриць блоків ЦЗ як у просторовій, так і в частотній області, тому формалізація процесу

стеганоперетворення у вигляді сукупності збурень СНЧ блоків не залежить від аналізованої області зображення (просторової, частотної).

СНЧ матриці є добре обумовленими. Найбільш яскраво особливості їх збурень при стиску проявляються для найменших СНЧ B: значення найменших СНЧ блоків зображення, збереженого у форматі із втратами, порівнянні з похибкою округлення й між собою, що не характерно для блоків ЦЗ, збереженого без втрат. Крім того, характер поведінки найменших СНЧ ($\sigma_6, \sigma_7, \sigma_8$) блоків зображень із втратами якісно відрізняється від характеру СНЧ із тими ж номерами для блоків зображень, збережених без втрат: швидкість їх зміни в першому випадку значно менше аналогічного параметра для другого випадку (рис.9.1).

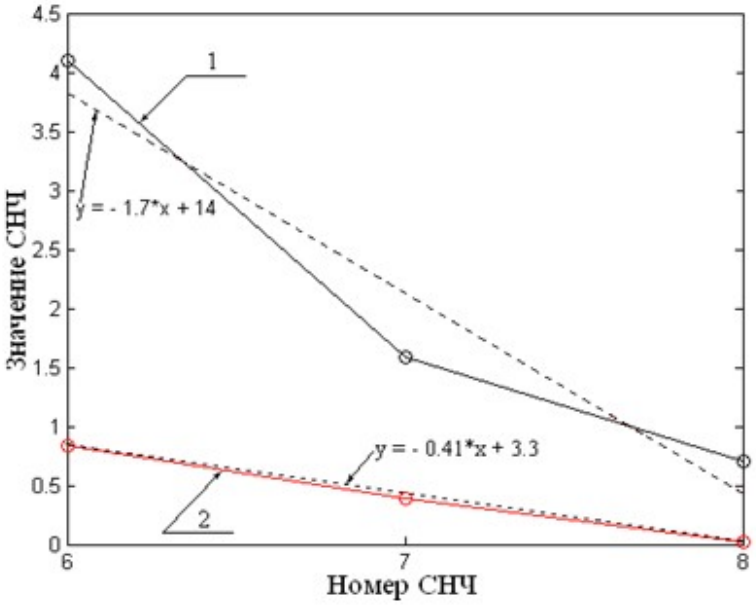


Рис.9.1. Типовий приклад графіків залежності значень найменших СНЧ $\sigma_6, \sigma_7, \sigma_8$ від їхніх номерів і їх лінійні апроксимації для 8×8 – блока: 1 — TIF-зображення; 2 — ЦЗ в форматі з втратами

Для побудови стеганографічного методу, стійкого до атаки стиском, важливими є наступні висновки:

- Збурення різних СНЧ у ході стиску, аналіз яких можна проводити як у частотній, так і в просторовій області зображення, порівнянні між собою і з величиною збурної дії (якщо враховувати оцінку зверху), тому, при формальному представленні результату процесу стеганоперетворення у вигляді сукупності збурень СНЧ ***для принципової можливості декодування секретної інформації сукупний результат збурень при вбудові ДІ повинен перевершувати збурення, яке буде перетерплювати блок стеганоповідомлення в процесі стиску***;
- не має сенсу задіювати найменші СНЧ при організації процесу стеганоперетворення, тому що після стиску незалежно від того, як збурювалися ці СНЧ при вбудові ДІ, вони стануть порівнянні між собою і з нулем, а вбудована в них інформація з великою ймовірністю буде загублена;
- СНЧ нечутливі до збурень (стиску). Однак, якщо стиск буде відбуватися з низькою якістю, що приведе до збільшення норми матриці збурення кожного блоку ЦЗ $\|\Delta B\|$, збурення в процесі стиску СНЧ також збільшаться, а це значить, що при стеганоперетворенні буде потрібно збільшення збурення СНЧ, які є формальним представленням вбудови ДІ, щоб «перекрити» «руйнуючу дію» стиску. Однак у результаті такого «перекриття» можливе виникнення двох негативних наслідків:

– Порушення надійності сприйняття стеганоповідомлення;

– Порушення первісного порядку СНЧ, що може значно утруднити (або навіть унеможливити) процес аналізу стеганоповідомлення, а також процес декодування ДІ у випадку, коли процес стеганоперетворення формалізований у вигляді сукупності збурень СНЧ.

Щоб уникнути порушення первісного порядку СНЧ, процес стеганоперетворення (з урахуванням можливості стиску стеганоповідомлення з низькими коефіцієнтами якості) достатньо проводити таким чином, щоб необхідні для «перекриття стиску» значні збурення зазнавали тільки максимальні СНЧ блоків σ_1 (і можливо σ_2): за рахунок великих величин значень їх відокремленостей $svdgap(i,B)$, що визначаються відповідно до формули $svdgap(i,B)=\min\limits_{i\neq j}\left|\sigma_j-\sigma_i\right|$ (табл.9.1), зміни їх взаємного порядку після стеганоперетворення можна легко уникнути. Припустима величина збурень максимальних СНЧ, що відбуваються в результаті вбудови ДІ, повинна бути встановлена з врахуванням вимоги дотримання надійності сприйняття формованого стеганоповідомлення.

Таблиця 9.1. Середні по зображенню відокремленості СНЧ блоків

№ЦЗ	Середнє значення $svdgap(i,B)$							
	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$
1	836.1147	4.1115	2.1272	1.5128	1.1007	0.7625	0.5039	0.6462
2	1480.0	15.4986	5.4764	2.5691	1.4726	0.8849	0.5374	0.6754
3	1035.3	46.3636	15.4570	4.6921	2.0874	1.0268	0.5674	0.7066
4	177.1812	12.1960	5.2092	3.1785	2.1130	1.4012	0.9200	1.1715
5	1242.2	4.9557	2.1623	1.3388	0.9123	0.6095	0.4069	0.5248
Ср.зн-е (200 ЦЗ)	712.4564	23.1111	7.9843	3.0004	1.4232	0.7125	0.4667	0.5781

Для одержання оцінки середнього збурення, яке зазнає блок матриці ЦЗ, збереженого без втрат, при стиску з різною якістю, достатньо провести обчислювальний експеримент. У ході експерименту зображення у форматі без втрат перезберігалися з коефіцієнтами якості $QF\in\{70,75,80,85,90,95\}$. При зменшенні QF величина збурної дії на блок при стиску ЦЗ зростає. Так, наприклад, при стиску з $QF=85$ найчастіше блок B ЦЗ зазнає збурення ΔB, спектральна норма матриці якого $\|\Delta B\|_2$ порядка 10, при цьому максимальне збурення $\|\Delta B\|_2\approx 40$. Якщо ж $QF=70$, то максимальне збурення блоку матриці ЦЗ досягає $\|\Delta B\|_2\approx 75$.

Таким чином, як показує обчислювальний експеримент, відокремленість максимального СНЧ σ_1 блоку вхідного ЦЗ, збереженого без втрат, у переважній більшості випадків буде значно більше максимального значення норми матриці збурення блоку при стиску. Звідси випливає, що процес стеганоперетворення для існування принципової можливості здійснення декодування ДІ може бути формалізований як сукупність збурень максимальних СНЧ блоків σ_1, переважаючих найбільше значення $\|\Delta B\|_2\approx 75$ (з урахуванням необхідної вимоги забезпечення надійності сприйняття стеганоповідомлення).

3. Стеганографічний метод, стійкий до атаки стиском

У якості контейнера для пропонованого нижче алгоритму може виступати як кольорове ЦЗ, так і зображення в градаціях сірого. Для кольорового ЦЗ вбудова ДІ буде

проводитися в одну з матриць R, G або B. Як ДІ розглядається послідовність $p_1, p_2, ..., p_t$, де $p_i \in \{0,1\}$, $i = 1,2,...t$.

Позначимо через K порогове значення варіації збурень максимальних СНЧ, зміст якого буде пояснений нижче. Тоді основні кроки пропонованого алгоритму виглядають у такий спосіб.

Вбудова ДІ.

Крок 1. Матриця F контейнера розбивається стандартним чином на блоки B розміром 8×8. Кожний блок використовується для вбудови 1 біта ДІ.

Крок 2. (*Вбудова 1 біта ДІ*). Нехай B - черговий блок, що використовується для стеганоперетворення, а p_i - черговий біт ДІ.

2.2. Побудувати сингулярне розкладання $B = U\Sigma V^T$, де $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_8)$;

2.3. ***Якщо***

$p_i = 0$

то

σ_1 коректується так, щоб різниця між σ_1, σ_2 при діленні на K давала залишок $K/4$. Результат коректування – збурене максимальне СНЧ $\overline{\sigma}_1$;

інакше

σ_1 коректується так, щоб різниця між σ_1, σ_2 при діленні на K давала залишок $3K/4$. Результат - $\overline{\sigma}_1$.

Крок 3. (*Формування блоку стеганоповідомлення* $\overline{F}$). Відповідний B блок стеганоповідомлення $\overline{B}$ обчислюється відповідно до формули:

$$\overline{B} = U\overline{\Sigma}V^T,$$

де $\overline{\Sigma} = diag(\overline{\sigma}_1, \sigma_2, ..., \sigma_8)$.

Декодування ДІ.

Крок 1. Матриця $\overline{F}$ стеганоповідомлення розбивається стандартним чином на блоки $\overline{B}$ розміром 8×8. Кожний блок використовується для декодування 1 біта ДІ.

Крок 2. (*Декодування біта ДІ*). Нехай $\overline{B}$ - черговий блок, з якого декодується біт p_i ДІ.

2.2. Побудувати сингулярне розкладання $\overline{B} = \overline{U}\overline{\Sigma}\overline{V}^T$, де $\overline{\Sigma} = diag(\overline{\sigma}_1, \overline{\sigma}_2, ..., \overline{\sigma}_8)$;

2.3. ***Якщо***

різниця $\overline{\sigma}_1 - \overline{\sigma}_2$ при діленні на K дає залишок менше $K/2$

то

$$p_i = 0;$$

інакше

$$p_i = 1.$$

Розглянемо порогове значення варіації збурень максимальних СНЧ K. Виходячи з наведених вище результатів, значну стійкість запропонованого алгоритму можна було б очікувати у випадку $K \geq 300$. Тоді залишки від ділення $\sigma_1 - \sigma_2$, наприклад, для $K = 300$, можуть приймати значення з множини $\{0,1,2,...,299\}$. При вбудові $p_i = 0$ СНЧ σ_1 чергового блоку стає таким, що залишок від ділення $\sigma_1 - \sigma_2$ на K дорівнює 75, для $p_i = 1$ згаданий залишок буде рівний 225 (рис.9.2). Виходячи з можливого максимального

збурення σ_1 при стиску з $QF \geq 70$ ($\max\|\Delta B\|_2 \approx 75$) і конкретики алгоритму декодування ДІ, стиск із $QF \geq 70$ з великою ймовірністю не зможе вивести значення СНЧ σ_1 за межі «зони», що відповідає вбудованому біту ДІ (рис.9.2). Однак, як показує обчислювальний експеримент, значення $K = 300$, що використовується в процесі стеганоперетворення, не завжди забезпечує надійність сприйняття стеганоповідомлення. Зауважимо, що хоча максимальне значення збурення блоку розглядалося як $\|\Delta B\|_2 \approx 75$, отримане для $QF = 70$, не має сенсу з'ясовувати максимальне значення $\|\Delta B\|_2$ для $QF < 70$: очевидно, що в цих випадках $\|\Delta B\|_2 > 75$, однак збільшення значення K у силу вищесказаного не представляється можливим.

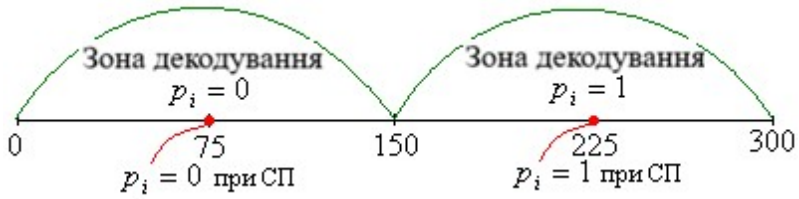


Рис. 9.2. Ілюстрація процесів вбудови й декодування ДІ при $K = 300$

Зменшення K до 250 не забезпечило надійність сприйняття стеганоповідомлення. Нарушение надежности восприятия отмечено не было при $K = 200$. Сформовані стеганоповідомлення спочатку зберігалися у форматі без втрат, а потім перезберігалися у формат Jpeg з різними коефіцієнтами якості, після чого відбувалося декодування ДІ.

Результати експериментів наведені в табл.9.2. Обсяг відновленої при декодуванні ДІ P обчислювався відповідно до формули:

$$P = \frac{k - \sum_{i=1}^{k} p_i \oplus \overline{p}_i}{k} \cdot 100\%,$$

де $\oplus$ - операция логического исключающего ИЛИ, $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, - декодированная из стеганосообщения ДИ.

Таблиця 9.2. Залежність обсягу відновленої при декодуванні ДІ від значення коефіцієнта якості QF

Формат збереження ЦЗ-контейнера	Середнє значення P при різних значеннях коефіцієнта якості QF, що використовувався при стиску стеганоповідомлення (%)		
	$QF = 95$	$QF = 70$	$QF = 30$
Tif	98.97	98.07	92.13
Jpeg	98.54	98.11	91.06

Як видно з результатів експерименту, ефективність запропонованого алгоритму не залежить від формату зберігання контейнера, а обсяг відновленої при декодуванні ДІ говорить про стійкість алгоритму до стиску навіть із малим коефіцієнтом якості $QF = 30$. Для більш повної ілюстрації експерименту служить рис.9.3.

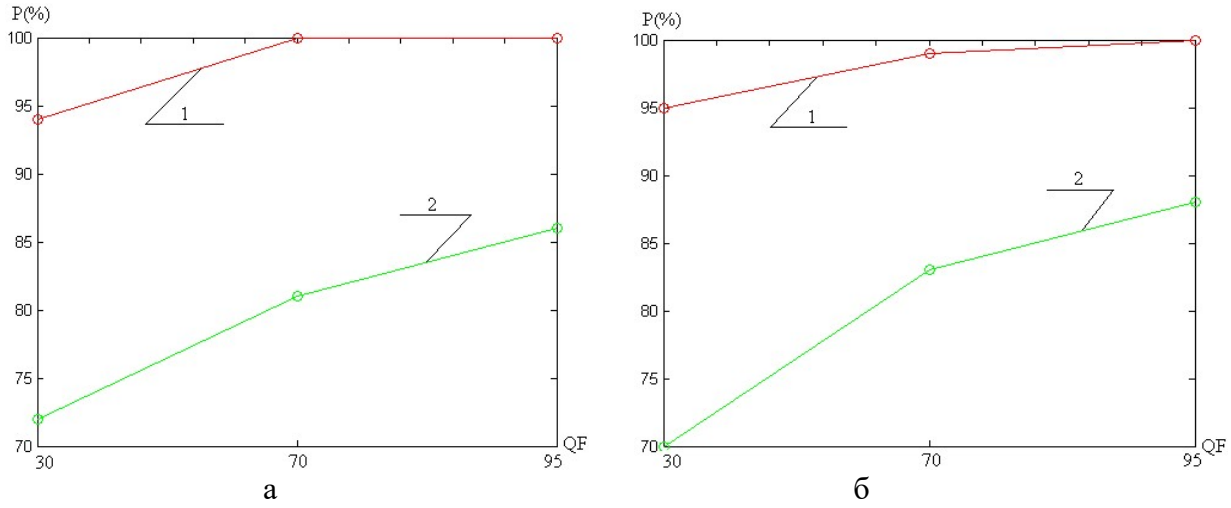


Рис.9.3. Залежність обсягу відновленої інформації від коефіцієнта якості QF для контейнерів, що зберігаються в форматі: а – Jpeg; б – Tif ; 1 – максимальне значення P по всім ЦЗ, що тестувалися; 2 – мінімальне значення P по всім ЦЗ, що тестувалися

Для відносної оцінки ефективності роботи стеганометоду, наведеного вище, було проведено його порівняння з методом Кахо й Жао (МКЖ), який також позиціонується як стійкий до стиску. Після стеганоперетворення отримане стеганоповідомлення зберігалося в Jpeg з $QF = 75,80,85,90,95$. Результаты представлені в табл.9.3.

Таблиця 9.3. Результати декодування секретної інформації в методі Коха й Жао при різних значеннях коефіцієнта якості QF

$(i_1, j_1), (i_2, j_2)$	QF	ОПИ (%)	Забезпечення надійності сприйняття стеганоповідомлення
(5,4), (4,5)	75	54.6339	+
	80	91.7782	+
	85	99.1146	+
	90	99.9362	+
	95	99.9947	+
(3,4), (4,3)	75	71.3798	+
	80	94.9230	+
	85	99.0976	+
	90	99.9126	+
	95	99.9782	+
(2,3), (3,2)	75	98.0660	-
	80	99.7319	-
	85	99.8848	-
	90	99.9132	-
	95	99.9392	-

Сравнивнение результатов, приведенных в табл. 9.2, 9.3, однозначно говорит в пользу предлагаемого СА (заметим, что относительная замена коэффициентов (2,3), (3,2), которые являются низкочастотными, не может рассматриваться в качестве практически используемого варианта МКЖ, т.к. приводит к нарушению надежности восприятия стеганосообщения).

Питання

1. Як в загальному вигляді можна представити довільне стеганоперетворення?
2. Чому формалізація процесу стеганоперетворення у вигляді сукупності збурень СНЧ блоків не залежить від аналізованої області зображення (просторової, частотної)?
3. Пояснити, чому для принципової можливості декодування секретної інформації сукупний результат збурень при вбудові ДІ повинен перевершувати збурення, яке буде перетерплювати блок стеганоповідомлення в процесі стиску.
4. Пояснити, чому не має сенсу задіювати найменші СНЧ блоків контейнеру при організації процесу стеганоперетворення.
5. Як має сенс проводити процес стеганоперетворення (з урахуванням можливості стиску стеганоповідомлення з низькими коефіцієнтами якості), щоб уникнути порушення первісного порядку СНЧ?
6. Основні кроки стеганографічного методу, стійкого до атаки стиском.

ЛІТЕРАТУРА

Базова

1. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних підручник. / Г.Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. –558 с.
2. Steganography - The Art of Hiding Information: The Art of Hiding Information. - BoD – Books on Demand, 2024. 160 p.
3. Abid Yahya. Steganography Techniques for Digital Images. Springer, 2018. – 122 p.
4. Компютерна стеганографія: навчальний посібник / В.О.Хорошко, Ю.Є.Яремчук, В.В.Карпінець – Вінниця: ВНТУ, 2017. – 155 с.

Допоміжна

1. Bobok I.I., Kobozeva A.A. Steganalysis method efficient for the hidden communication channel with low capacity. *Радіотехніка*. 2019. 198. С. 19–31.
2. Kobozieva at al. Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel/ PROBLEMELE ENERGETICII REGIONALE. 2(66). 2025. Pp.90-104
3. Кобозєва А.А., Бобок І.І. Локалізація області збурень формальних параметрів стеганографічного контейнера для забезпечення стійкості стеганосистеми/ Вісті вищих учбових закладів. Радіоелектроніка Т.67, № 8.
4. Кобозєва А.А., Бобок І.І. Стеганоаналітичний метод виявлення LSB-вкладень в цифровому відео, послідовності цифрових зображень / Обробка інформації в системах управління та прийняття рішень. Проблеми та рішення. Монографія / Аксак Н., Бобок І. і др.; під наук. ред. проф. В.Вичужаніна –Одеса: НУ «ОМА», 2023 – 358 с.
5. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. Radiotekhnika. 2021. 4(207). P. 27–39.

Інтернет ресурси

1. https://api.pageplace.de/preview/DT0400.9781139574648_A23868110/preview-9781139574648_A23868110.pdf
2. https://ceur-ws.org/Vol-3513/
3. https://journal.ie.asm.md/ru/contents/electronni-jurnal-254-2022