Міністерство освіти та науки України

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

КОНСПЕКТ ЛЕКЦІЙ
(частина 1)
з дисципліни
«ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ПІДХОДИ ДО ЇХ ВИРІШЕННЯ»
для здобувачів другого (магістерського) рівня вищої освіти
специальності 125 - Кібербезпека

Одесса, 2021

Міністерство освіти та науки України

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

КОНСПЕКТ ЛЕКЦІЙ
(частина 1)
з дисципліни
«ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ПІДХОДИ ДО ЇХ ВИРІШЕННЯ»
для здобувачів другого (магістерського) рівня вищої освіти
специальності 125 - Кібербезпека

Затверджено
на засіданні кафедри КБПЗ
Протокол № 1 від 27.08.2021 р.

Одеса, 2021

Конспект лекцій (частина 1) з дисципліни «Проблеми кібербезпеки та сучасні підходи до їх вирішення» для здобувачів другого (магістерського) рівня вищої освіти специальності 125 – Кібербезпека / Укл.: А.А.Кобозєва. – Одеса: «Одеська політехніка», 2021. - 119 с.

Укладач: проф. Кобозєва А.А.

ЗМІСТ

ПЕРЕДМОВА 5
Лекція 1 6
Лекція 2 13
Лекція 3 .....
Лекція 4 26
Лекція 5 31
Лекція 6 37
Лекція 7 43
Лекція 8 52
Лекція 9 57
Лекція 10 63
Лекція 11 70
Лекція 12 77
Лекція 13 81
Лекція 14 101
Лекція 15 110

ПЕРЕДМОВА

Дисципліна «Проблеми кібербезпеки та сучасні підходи до їх вирішення» відповідає освітньо-професійній програмі, навчальному та робочому плану підготовки фахівців другого (магістерського) освітньо-професійного рівня вищої освіти за спеціальністю 125 Кібербезпека, і є складовою циклу дисциплін професійної підготовки обов'язкової частини навчального плану.

Предмет дисципліни «Проблеми кібербезпеки та сучасні підходи до їх вирішення» – процеси аналізу кіберзахищеності та синтезу захищених інформаційних систем з використанням сучасних, зокрема авторських, математичних підходів.

Метою дисципліни є забезпечення розвитку фахових компетентностей майбутніх магістрів шляхом оволодіння сучасними підходами до вирішення проблем кібербезпеки.

Завдання вивчення дисципліни:

- Формування у здобувачів загального універсального теоретичного базису для розв'язку різноманітних сучасних проблем в інформаційній та кібербезпеці;
- Набуття практичних навичок застосування теоретичних знань для вирішення конкретних задач, зокрема, в стеганографії, стеганоаналізі, криптографії, виявлення порушень критеріїв захищеності інформації, зокрема її цілісності, що відбувається різноманітними шляхами, в тому числі за допомогою існуючих програмних засобів, програмних середовищ, графічних редакторів, тощо.

Стратегічні цілі дисципліни – націлити майбутніх фахівців на творче застосування, розвиток, удосконалення отриманих знань у подальшій професійній підготовці та їх наступній практичній діяльності.

СЕМЕСТРОВИЙ МОДУЛЬ 1

Змістовий модуль 1. ЗАГАЛЬНИЙ ПІДХІД ДО АНАЛІЗУ СТАНУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Лекція 1. ЗАГАЛЬНА МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ІНФОРМАЦІЙНОГО ПРОЦЕСУ

План

1. Вступ
2. Поняття чутливості задачі
3. Формальне представлення інформаційної системи та її перетворення

1. Вступ

Процес впровадження нових інформаційних технологій в усі сфери життя суспільства неможливий без розв'язку питань інформаційної безпеки, яка структурується в зовсім різних, але зв'язаних між собою аспектах. Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем, перехід до безпаперової технології, збільшення обсягів оброблюваної інформації й розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даним інформаційних систем (ІС), до їхньої високої вразливості. У сучасних умовах, що вимагають захисту не тільки державної й військової, але й промислової, комерційної, фінансової таємниць, захист інформації в цілому й захист інформації в автоматизованих ІС зокрема стає усе більш складною проблемою, вимагає для свого розв'язку залучення сучасних наукових вишукувань і результатів дослідження.

Теоретичні основи побудови систем захисту інформації дуже складні й, незважаючи на інтенсивність досліджень у цій предметній області, далекі від досконалості.

Напрацьований в області інформаційної безпеки математичний апарат, що включає в якості інструментів теорію ймовірностей, дискретну математику, теорію нечіткихмножин, нечітку логіку, штучні нейронні мережі і т.д., виявився недостатнім для опису об'єктів, які погано формалізуються, мають властивості, погано відомі апріорі й мінливі в процесі функціонування, якою є будь-яка ІС.

Новим і надзвичайно перспективним є підхід до проблеми аналізу стану й створення систем захисту інформації, заснований на теорії збурень і матричному аналізі, який дає можливість для визначення чутливості довільного об'єкта до змін вхідних даних, ступеня залежності стану об'єкта від збурних дій для апріорної оцінки властивостей об'єкта.

2. Поняття чутливості задачі

При розв'язку довільної задачі в загальному випадку неможливо одержати точне значення шуканого чисельного результату. Існування неусувної похибки в математичній моделі об'єкта або процесу, що фігурує в задачі (математичний опис задачі є неточним), погрішності вхідних даних, багато з яких у реальних умовах отримані експериментально, погрішність методу, використовуваного для розв'язку, і обчислювальна, погрішності, що виникають при яких-небудь додаткових впливах на об'єкт, які часто трактуються як збурення вхідних даних, приводять до необхідності їх сукупного врахування при оцінці погрішності результату. Навіть у випадку, коли вхідні дані математичної моделі не мають погрішностей, а метод, обраний для розв'язку отриманої математичної задачі є точним, уникнути обчислювальної погрішності при проведенні обчислень у системі чисел із плаваючою точкою, а тому і погрішності в отриманому результаті, неможливо. Після побудови математичної моделі реального процесу, яка необхідно задовольняє вимозі адекватності (розв'язок математичної задачі, отриманий з її допомогою, незначно відрізняється від дійсного розв'язку реальної задачі), вхідна задача і її математична формалізація в процесі розв'язку й аналізу отриманого результату, як правило, не розділяються. Однак, у силу особливостей машинної арифметики, неможливо в загальному випадку одержати точний

розв'язок навіть змодельованої математичної задачі (припускаючи навіть відсутність неусувної погрішністю й погрішністю методу).

Отриманий наближений (у силу перерахованих вище причин) розв'язок деякої обчислювальної задачі A може розглядатися як точний розв'язок, але іншої, збуреної задачі $\overline{A}$ ($\overline{A}$ відрізняється від A збуренням вхідних даних). У цьому випадку для визначення якості отриманого наближення необхідно мати можливість оцінити ступінь залежності розв'язку від збурень вхідних даних.

Деякі обчислювальні задачі дуже сильно «реагують» на навіть малі зміни даних, причому це не залежить від системи із плаваючою точкою або обраного алгоритму, а є властивістю самої задачі.

Для кращого розуміння поняття чутливості задачі розглянемо деякі приклади.

Приклад. Розглянемо квадратне рівняння, корені якого є «майже» кратними:

$$(x-2)^2 = 10^{-6}.$$

Корені рівняння: $x = 2 \pm 10^{-3}$. Зміна правої частини рівняння лише на 10^{-6} приведе до зміни коренів на 10^{-3}, тобто на три порядки більше, ніж початкова. Ця задача є чутливою.

Задача називається чутливою до погрішностей вхідних даних, якщо навіть малі погрішності вхідних даних можуть привести до значної (значно більшої) погрішності результату, і нечутливою інакше.

Для чутливих задач «правильні» відповіді (відповіді з дуже малою погрішністю) принципово не можна одержати ніяким алгоритмом, оскільки навіть малі помилки, допущені при представленні даних і при обчисленнях (а ці помилки супроводжують обчислювальний процес завжди) приведуть до значних (значно більших) погрішностей у результатах. У силу цього надзвичайно важливою й актуальною є чисельна оцінка такої чутливості, встановлення параметрів, що визначають чутливість, достатніх умов нечутливості задачі.

Якщо задача є чутливою до збурних дій, то навіть незначні зміни вхідних даних (малі збурні дії) сильно змінять результат її розв'язку. Якщо ж задача нечутлива, то малі «збої» вхідних даних на самому об'єкті не відіб'ються (відіб'ються незначно)

Нехай ξ — вхідні дані для деякої задачі, результатом рішення якої є $\phi(\xi)$; $\overline{\xi}$ — збурені вхідні дані, а рішення задачі, отримане для цих вхідних даних, — $\phi(\overline{\xi})$. Числом обумовленості задачі називається величина, що визначається як:

$$\overline{\lim_{\overline{\xi} \to \xi}} \frac{\textit{відстань між } \phi(\xi) \textit{ і } \phi(\overline{\xi})}{\textit{відстань між } \xi \textit{ і } \overline{\xi}}.$$

(1.1)

Відстані, що фігурують у формулі (1.1), визначаються введенням відповідних метрик у просторах вхідних даних і результатів. Необхідно відзначити, що за змістом співвідношення (1.1) представляє із себе деякий аналог абсолютного значення швидкості зміни функції результату в точці ξ.

Очевидно, чим менше число обумовленості, тим менше збурення результату залежить від збурення вхідних даних, тим менше чутливість задачі, а при малому числі обумовленості задача виявиться нечутливою до погрішностей вхідних даних. Таким чином, число обумовленості задачі є її мірою чутливості до збурних дій.

Приклад. Розв'язати систему рівнянь:

$$\begin{cases} 0.780x + 0.563y = 0.217, \\ 0.457x + 0.330y = 0.127. \end{cases}$$

Припустимо, що обчислення проводяться в системі із плаваючою точкою, для якої основа система числення $\beta = 10$, а кількість розрядів в мантисі $t = 3$. Розв'язуючи систему методом Гаусса, одержимо:

$$x = 1.71, \quad y = -1.98.$$

При підстановці розв'язку у вхідну систему одержимо:

$$\begin{cases} 0.780 \cdot 1.71 + 0.563 \cdot (-1.98) - 0.217 = 0.00206 \approx 0, \\ 0.457 \cdot 1.71 + 0.330 \cdot (-1.98) - 0.127 = 0.00107 \approx 0. \end{cases}$$

І хоча підстановка показала «гарний результат», точний розв'язок системи, насправді, дорівнює:

$$x = 1.00, \quad y = -1.00.$$

Обчислений розв'язок дуже відрізняється від точного. Розглянута задача є чутливою (або погано обумовленоюї, або некоректно поставленою).

Визначення. Чутливістю ІС назвемо чутливість задачі її формування.

3. Формальне представлення інформаційної системи та її перетворення

Можна показати, що довільний інформаційний процес (ІП) (чи ІС, що розглядається як результат процесу її синтеза) може бути формально представлений в вигляді скінченної множини матриць $M_1, M_2, \ldots, M_m$ певної скінченної вимірності з дійсними елементами, а тому аналіз будь-якого ІП (ІС) принципово можна звести до аналізу відповідних матриць.

Як показує практика, з урахуванням зручності обробки одержуваної моделі, найчастіше при моделюванні реальних процесів і об'єктів використовуються двовимірні матриці, які й будуть розглядатися далі при описі ІС.

Твердження. Будь-який ІП (ІС) може бути формально представлений у вигляді скінченної множини двовимірних дійсних матриць, а тому формальний аналіз процесу принципово можна звести до аналізу двовимірних матриць.

Для спрощення викладу, не обмежуючи при цьому спільності міркувань, у якості математичної моделі ІС будемо розглядати двовимірну (прямокутну або квадратну) матрицю F.

Результат будь-яких дій над ІС, що моделюється, у загальному випадку можна представити як збурення ΔF матриці F, самі дії — збурні дії на F, а завдання будь-якого перетворення системи, тобто генерації нової, для якої стара є вхідними даними, - це завдання одержання збуреної матриці для вхідної матриці F, до того ж результуюча матриця очевидно задовольняє співвідношенню:

$$\overline{F} = F + \Delta F, \qquad (1.2)$$

де $\Delta F = f(F)$, тобто ΔF є деякою функцією матриці F.

Таким чином, зі співвідношення (1.2) випливає наступне

Твердження. Будь-які перетворення довільної ІС можуть бути формально представлені у вигляді елементарних матричних операцій.

Таким чином, у якості набору формальних параметрів, що однозначно визначають й всебічно характеризують будь-яку ІС, 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 $f_{ij}, i = \overline{1,m},\ j = \overline{1,n}$, ($m \geq n$). Для неї має місце представлення, що називається сингулярним розкладанням (SVD):

$$F = U \Sigma V^T, \tag{1.3}$$

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 і 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.)

У загальному випадку SVD матриці визначається неоднозначно.

Вектор u називається лексикографічно додатним, якщо його перший ненульовий компонент додатний, а SVD (1.3) нормальним, якщо стовпці матриці U лексикографічно додатні. Можна показати, що невироджена матриця має єдине нормальне SVD, якщо її СНЧ попарно різні. Далі будемо вважати, що всі матриці, які розглядаються, мають таку властивість. Таким чином, СНЧ і сингулярні вектори (СНВ), одержувані нормальним SVD, однозначно визначають матрицю, а значить можуть розглядатися як повний набір параметрів для ІС. Далі, говорячи про СНВ, будемо припускати, що вони ортонормовані лексикографічно додатні, тобто такі, які однозначно визначаються нормальним SVD.

Будь-яке перетворення ІС збурить її матрицю F, а значить певним чином збурить її СНЧ і СНВ. Тому має місце наступне

Твердження. Будь-яке перетворення ІС може бути формально представленим у вигляді сукупності збурень СНЧ і (або) СНВ її матриці, що дозволяє природно звести задачу аналізу процесу перетворення й підсумкового стану системи до аналізу збурень СНЧ і СНВ, а задачу синтезу системи із заданими властивостями - до задачі забезпечення певних характеристик збурень СНЧ і СНВ її матриці.

Таким чином, про результат перетворення ІС, її властивості, у тому числі й про одну з найбільш важливих властивостей - чутливість, можна судити по характерних рисах сукупності збурень однозначно визначальних її параметрів - СНЧ і СНВ.

Для СНЧ $\sigma_j(F),\ \sigma_j(F + \Delta F),\ j = \overline{1,n}$, матриць F і $F + \Delta F$ відповідно має місце співвідношення:

$$\max_{1 \leq j \leq N} \left| \sigma_j(F) - \sigma_j(F + \Delta F) \right| \leq \left\| \Delta F \right\|_2, \tag{1.4}$$

де $\|\bullet\|_2$ — спектральна матрична норма (СМН).

Відокремленістю СНЧ σ_i матриці F називається величина:

$$svdgap(i,F) = \min_{i \neq j} \left| \sigma_j - \sigma_i \right|.$$

Нехай θ_i — кут між відповідними вхідним і збуреним сингулярними векторами u_i і $\bar{u}_i$, тоді мають місце співвідношення:

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F)} \text{ за умови } svdgap(i,F) \neq 0, \quad (1.5)$$

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F+\Delta F)} \text{ за умови } svdgap(i,F+\Delta F) \neq 0. \quad (1.6)$$

Таким чином, виходячи з (1.5), (1.6),реакція СНВ матриці на збурну дію буде різною навіть у межах однієї матриці, вона буде залежати від значення відокремленості відповідного СНЧ: чим більше відокремленість СНЧ, тим менш чутливим до збурних дій буде відповідний СНВ.

У силу співвідношення (1.4) збурення СНЧ порівнянні зі збуренням даних — ΔF, тобто СНЧ матриці є нечутливими до збурних дій незалежно від того, чутливою або нечутливою виявиться розглянута задача по формуванню $F + \Delta F$, тобто задача перетворення ІС.

Зауваження. Для оцінки чутливості задачі перетворення ІС із матрицею F має сенс аналізувати лише збурення СНВ F, що відбулися в результаті перетворення.

Результат перетворення системи для встановлення міри чутливості до збурних дій будемо розглядати у вигляді сукупності збурень СНВ її матриці.

Твердження. Чутливість задачі, що полягає в довільному перетворенні ІС, математичною моделлю якої є двовимірна матриця, буде визначатися чутливістю збурених перетворенням системи СНВ матриці.

Розглянемо другий можливий повний набір параметрів.

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:

$$F = U \Lambda U^T \quad (1.7)$$

де $\Lambda = diag(\lambda_1,...,\lambda_n)$ — матриця ВЗ;

$U = [u_1,...,u_n]$ — матриця ВВ.

Розкладання (1.7) може бути представлено у формі зовнішніх добутків:

$$F = \sum_{i=1}^{n} \lambda_i u_i u_i^T. \quad (1.8)$$

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 ВВ.

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

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

Далі будемо вважати, що всі симетричні матриці, що розглядаються, задовольняють умові попередньої теореми.

Для ІС, моделлю якої є симетрична матриця, має місце твердження:

Твердження. Будь-яке перетворення ІС у випадку симетричності її матриці представляється у вигляді збурень спектра й (або) ВВ матриці, що однозначно визначаються нормальним СР, що дозволяє звести задачу аналізу процесу перетворення й підсумкового стану ІС до аналізу збурень ВЗ і ВВ, а задачу синтезу системи із заданими властивостями - до забезпечення певних характеристик збурень ВЗ і ВВ її матриці.

Для ВЗ симетричної матриці має місце оцінка, аналогічна (1.4):

$$\max_{1 \leq j \leq n} |\lambda_j(F) - \lambda_j(F + \Delta F)| \leq \|\Delta F\|_2, \qquad (1.9)$$

з якої випливає, що ВЗ симетричної матриці є добре обумовленими, тобто нечутливими до збурних дій, чого не можна стверджувати в загальному випадку для несиметричних матриць.

Чутливість ВВ u_i, який відповідає ВЗ λ_i, в межах матриці F визначається відповідно до співвідношень:

$$\sin\theta_i \leq \frac{2\|\Delta F\|_2}{gap_{abs}(i,F)}, \qquad (1.10)$$

$$\sin\theta_i \leq \frac{2\|\Delta F\|_2}{gap_{abs}(i,\overline{F})}, \qquad (1.11)$$

$\overline{u_i}$ — нормований збурений ВВ,

θ_i — гострий кут між u_i і $\overline{u_i}$,

$$gap_{abs}(i,F) = \min_{i \neq j} \|\lambda_j| - |\lambda_i\| \qquad (1.12)$$

— абсолютна відокремленість ВЗ λ_i матриці F.

Твердження. Абсолютна відокремленість ВЗ матриці є мірою чутливості відповідного ВВ до збурних дій.

Виходячи з (1.9), маємо:

Твердження. Чутливість задачі, що полягає в довільному перетворенні ІС, математичною моделлю якої є симетрична матриця, буде визначатися чутливістю збурених перетворенням системи ВВ її матриці.

У силу співвідношення (9) збурення ВЗ (як і СНЧ) порівнянні зі збуренням даних — ΔF, ВЗ симетричної матриці є нечутливими до збурних дій незалежно від того, чутливою чи нечутливою виявиться розглянута задача по формуванню $F + \Delta F$.

Зауваження. Для оцінки чутливості задачі перетворення ІС із симетричною матрицею F має сенс аналізувати лише збурення ВВ F, що відбулися в результаті перетворення. Результат перетворення ІС для встановлення міри її чутливості до збурних дій будемо розглядати у вигляді сукупності збурень ВВ відповідної матриці.

Сингулярне і спектральне розкладання матриці пов'язані між собою.

Питання

1. В чому полягають труднощі при створенні теоретичного базису побудови систем захисту інформації?
2. Що таке чутливість інформаційної системи?
3. Формальне представлення інформаційної системи та її перетворення.
4. Пояснити, чому будь-які перетворення інформаційної системи, зокрема системи захисту інформації, можна представити у вигляді елементарних матричних операцій.
5. Що таке сингулярне розкладання матриці? Коли сингулярне розкладання визначається однозначно?
6. Збурення яких формальних параметрів ситеми має сенс аналізувати для оцінки її чутливості до збурних дій? Чому?
7. Чим визначається чутливість задачі, яка полягає в довільному перетворенні інформаційної ситеми? Пояснити.
8. Обумовленість сингулярних чисел (власних значень) , сингулярних векторів (власних векторів) матриці.

Література.

1. Козюра В.Д., Хорошко В.О., Шелест М.Є. Аналіз кібернетичної безпеки інформаційного суспільства. Інформаційна безпека людини, суспільства, держави. 2017. No 1 (21). – С.163-170. https://scholar.google.com.ua/citations?view_op=view_citation&hl=ru&user=Xt2Q-iwAAAAJ&cstart=20&pagesize=80&citation_for_view=Xt2Q-iwAAAAJ:IUKN3-7HHlwC
2. Прокофьєв М.І., Хорошко В.О. Проблеми захисту інформації в Україні. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (30), 2015 р. – С. 9-14. https://ela.kpi.ua/bitstream/123456789/18027/1/30_p9.pdf
3. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
4. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. - К.: Вид. ДУІКТ, 2010. – 316 с. http://www.dut.edu.ua/ru/lib/112/category/730/view/774
5. Гантмахер Ф.Р. Теория матриц: монография. 5-е изд. М.: Физматлит, 2004. 559 с. http://lib.brsu.by/sites/default/files/books/%D0%93%D0%B0%D0%BD%D1%82%D0%BC%D0%B0%D1%85%D0%B5%D1%80%20%D0%A4.%D0%A0.%20-%20%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F%20%D0%BC%D0%B0%D1%82%D1%80%D0%B8%D1%86.pdf

Лекція 2. ЗАГАЛЬНА МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ІНФОРМАЦІЙНОГО ПРОЦЕСУ (продовження)

План

1. Зв'язок між сингулярним і спектральним розкладаннями матриці системи
2. Зведення формального представлення інформаційної системи до симетричної матриці

1. Зв'язок між сингулярним і спектральним розкладаннями матриці

Сингулярне розкладання матриці A загального виду тісно пов'язане зі спектральними розкладаннями симетричних матриць

$$A^T A,\ AA^T,\ \begin{pmatrix} 0 & A^T \\ A & 0 \end{pmatrix}.$$

Твердження 1. Нехай $A = U\Sigma V^T$ - сингулярне розкладання $n \times n$-матриці A. Якщо A симетрична матриця з ВЗ λ_i і ВВ $u_i,\ i = \overline{1,n}$, тобто $A = U\Lambda U^T$ - спектральне розкладання A, то в сингулярному розкладанні матриці A $\sigma_i = |\lambda_i|$, $v_i = sign(\lambda_i)u_i$, при цьому $sign(0) = 1$.

Твердження 2. Нехай $A = U\Sigma V^T$ сингулярне розкладання $n \times n$-матриці A. Власними значеннями симетричної матриці $A^T A$ є σ_i^2, а праві СНВ v_i A — ортонормовані ВВ $A^T A$.

Доказ. Для матриці $A^T A$ має місце співвідношення:

$$A^T A = \left(U\Sigma V^T\right)^T U\Sigma V^T = V\Sigma^2 V^T \quad (1.13)$$

Рівність (1.13) очевидно представляє спектральне розкладання матриці $A^T A$, до того ж v_i — її ВВ, а діагональні елементи Σ^2 — ВЗ.

Твердження 3. Нехай $A = U\Sigma V^T$ сингулярне розкладання $n \times n$-матриці A. Власними значеннями симетричної матриці AA^T є σ_i^2. Ліві СНВ u_i — ортонормовані ВВ AA^T, що відповідають ВЗ σ_i^2.

Доказ. Аналогічний доказу твердження 2.

Твердження 4. Нехай $H = \begin{pmatrix} 0 & A^T \\ A & 0 \end{pmatrix}$, де A — квадратна $n \times n$-матриця, до того ж $A = U\Sigma V^T$ є сингулярне розкладання A. Тоді $2n$ ВЗ матриці H — це числа $\pm\sigma_i$, а відповідні нормовані ВВ мають вид $\frac{1}{\sqrt{2}}\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix}$.

Доказ. Оскільки матриця H симетрична, то

$$H^T H = H^2 = \begin{pmatrix} 0 & A^T \\ A & 0 \end{pmatrix}\begin{pmatrix} 0 & A^T \\ A & 0 \end{pmatrix} = \begin{pmatrix} A^T A & 0 \\ 0 & AA^T \end{pmatrix}.$$

(1.14)

З (1.14) випливає, що $H^T H$ — блочно-діагональна матриця, а тому її спектр є об'єднанням спектрів блоків. Спектри блоків $A^T A$, AA^T — це $\sigma_i^2, i = \overline{1,n}$. Позначимо спектральне розкладання матриці H

$$H = U_H \Lambda_H U_H^T.$$

Оскільки

$$H^2 = U_H \Lambda_H U_H^T U_H \Lambda_H U_H^T = U_H \Lambda_H^2 U_H^T,$$

(1.15)

тобто (1.15) — спектральне розкладання H^2, то ВЗ H^2 — це квадрати ВЗ H, а тому $2n$ ВЗ H визначаються як $\pm\sqrt{\sigma_i^2} = \pm\sigma_i$, и перша частина твердження доведена.

Для доказу другої частини перевіримо безпосередньо, що вектор $\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix}$ є ВВ матриці H:

$$H\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix} = \begin{pmatrix} 0 & A^T \\ A & 0 \end{pmatrix}\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix} = \begin{pmatrix} \pm A^T u_i \\ A v_i \end{pmatrix}.$$

(1.16)

Розглянемо складові правої частини (1.16):

$$A^T u_i = V\Sigma U^T u_i = V\Sigma \begin{pmatrix} u_1^T \\ \vdots \\ u_i^T \\ \vdots \\ u_n^T \end{pmatrix} u_i = V\Sigma \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = V \begin{pmatrix} 0 \\ \vdots \\ \sigma_i \\ \vdots \\ 0 \end{pmatrix} = \sigma_i v_i.$$

(1.17)

Аналогічно (1.17) показує, що

$$A v_i = \sigma_i u_i.$$

(1.18)

Враховуючи (1.17) і (1.18), з (1.16) випливає

$$H\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix} = \begin{pmatrix} \pm\sigma_i v_i \\ \sigma_i u_i \end{pmatrix} = \pm\sigma_i \begin{pmatrix} v_i \\ \pm u_i \end{pmatrix},$$

із чого за визначенню випливає, що $\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix}$ — ВВ матриці H, що відповідає ВЗ $\pm\sigma_i$, який після нормування стає рівним $\frac{1}{\sqrt{2}}\begin{pmatrix} v_i \\ \pm u_i \end{pmatrix}$.

Спираючись на встановлений зв'язок між сингулярним і спектральним розкладаннями відповідних матриць, можна перетворити алгоритми розв'язку симетричної проблеми ВЗ в алгоритми обчислення сингулярного розкладання. Це перетворення виконується не прямолінійно, оскільки сингулярне розкладання має додаткову структуру, яка часто може бути використана для підвищення ефективності й точності алгоритмів.

Для $n=3$ геометричне представлення довільного перетворення ІС у випадку рішення задачі чутливості подане на рис.1, де u_1, u_2, u_3 — СНВ (ВВ) матриці поданої системи, $\bar{u}_1, \bar{u}_2, \bar{u}_3$ — СНВ (ВВ) матриці збуреної ІС.

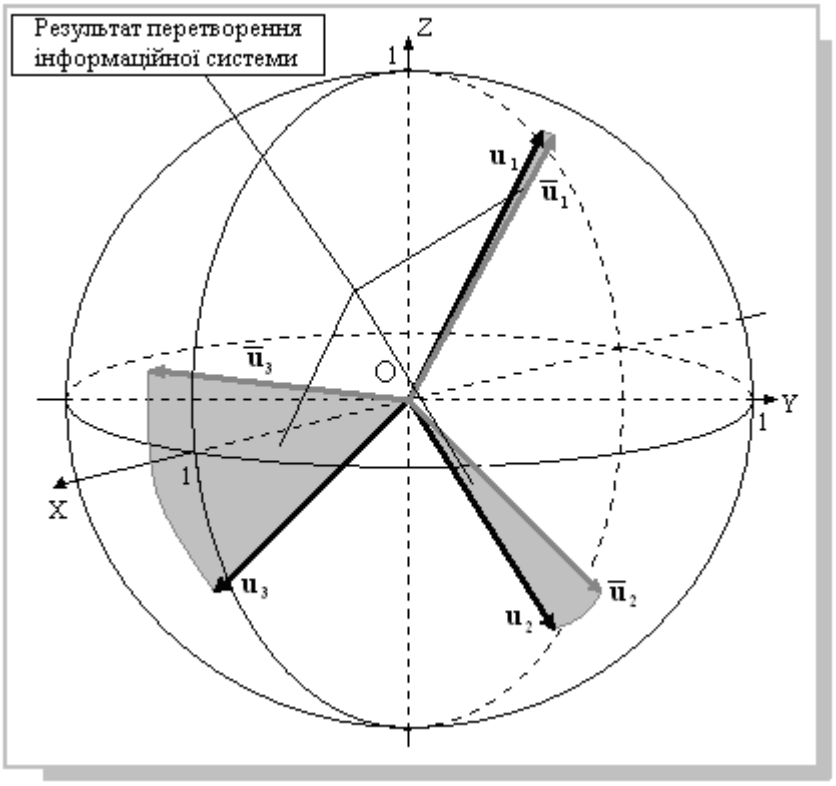


Рис.2.1. Геометричне представлення довільного перетворення інформаційної системи

2. Зведення формального представлення інформаційної системи до симетричної матриці

Нехай матриця F симетрична. Тоді в якості визначального її повного набору параметрів можна використовувати, як показано вище, як множину СНЧ і СНВ, так і спектр матриці й множину ВВ спеціального виду. Перевагу в цьому випадку слід віддати другому набору параметрів у силу наступних зауважень:

- побудова СР симетричної матриці має ряд переваг в обчислювальному сенсі в порівнянні з побудовою сингулярного розкладання для матриці довільної структури того ж розміру й того ж рівня заповнення;

- при цьому ВЗ симетричної матриці, як і її сингулярні числа, є добре обумовленими відповідно до (1.9), а ВВ, як і СНВ можуть бути в межах одної матриці як добре, так і погано обумовленими, що залежить від відокремленості відповідних ВЗ (СНЧ).

Однак, як правило, на практиці матриця ІС не задовольняє властивості: $F = F^T$. Поставимо у відповідність довільній F дві симетричні матриці $A,\ B$ того ж розміру за наступним правилом:

$$F = \begin{pmatrix} a_{11}\, a_{12}\ a_{13} \ldots a_{1n} \\ a_{21}\, a_{22}\ a_{23} \ldots a_{2n} \\ a_{31}\, a_{32}\ a_{33} \ldots a_{3n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1}\, a_{n2}\ a_{n3} \ldots a_{nn} \end{pmatrix} \rightarrow A = \begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{1n} \\ a_{12}\, a_{22}\, a_{23} \ldots a_{2n} \\ a_{13}\, a_{23}\, a_{33} \ldots a_{3n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{1n}\, a_{2n}\, a_{3n} \ldots a_{nn} \end{pmatrix}, B = \begin{pmatrix} a_{11}\, a_{21}\, a_{31} \ldots a_{n1} \\ a_{21}\, a_{22}\, a_{32} \ldots a_{n2} \\ a_{31}\, a_{32}\, a_{33} \ldots a_{n3} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1}\, a_{n2}\, a_{n3} \ldots a_{nn} \end{pmatrix}, \quad (1.19)$$

які будемо розглядати як симетричні матриці ІС. Це ніяк не обмежує міркувань у силу наступного. Нехай ΔF — матриця довільного збурення, яке зазнає F (або $\overline{F}$). В загальному випадку $\Delta F \neq \Delta F^T$. Матриці ΔF поставимо в співвідношення дві симетричні матриці того ж розміру, використовуючи правило (1.19), розглядаючи матрицю, що відповідає верхньому (нижньому) трикутнику ΔF як матрицю збурення для F ($\overline{F}$), яка отримана на основі $A(B)$, що дає принципову можливість матрицю довільного збурення й, як наслідок, матрицю $\overline{F}$ також розглядати як симетричні.

Будь-які збурення матриці F представляються в вигляді збурень верхнього (нижнього) трикутника матриці $A(B)$ с наступним симетричним відображенням результату відносно головної діагоналі $A(B)$. Нехай підсумком такого збурення є симетричні матриці $\overline{A}$ і $\overline{B}$. При остаточному формуванні матриці $\overline{F}$ використовується верхній трикутник $\overline{A}$ і нижній трикутник матриці $\overline{B}$.

Питання

1. Як повязані сингулярне і спектральне розкладання симетричної матриці?
2. Геометричне представлення довільного перетворення інформаційної системи.
3. Яким чином відбувається зведення формального представлення інформаційної системи до симетричної матриці? Які переваги дає симетричний вигляд матриці інформаційної системи?

Література.

6. Козюра В.Д., Хорошко В.О., Шелест М.Є. Аналіз кібернетичної безпеки інформаційного суспільства. Інформаційна безпека людини, суспільства, держави. 2017. No 1 (21). – С.163-170. https://scholar.google.com.ua/citations?view_op=view_citation&hl=ru&user=Xt2Q-iwAAAAJ&cstart=20&pagesize=80&citation_for_view=Xt2Q-iwAAAAJ:IUKN3-7HHlwC
7. Прокофьєв М.І., Хорошко В.О. Проблеми захисту інформації в Україні. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (30), 2015 р. – С. 9-14. https://ela.kpi.ua/bitstream/123456789/18027/1/30_p9.pdf
8. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.

9. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. - К.: Вид. ДУІКТ, 2010. – 316 с. http://www.dut.edu.ua/ru/lib/112/category/730/view/774
10. Гантмахер Ф.Р. Теория матриц: монография. 5-е изд. М.: Физматлит, 2004. 559 с. http://lib.brsu.by/sites/default/files/books/%D0%93%D0%B0%D0%BD%D1%82%D0%BC%D0%B0%D1%85%D0%B5%D1%80%20%D0%A4.%D0%A0.%20-%20%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F%20%D0%BC%D0%B0%D1%82%D1%80%D0%B8%D1%86.pdf

Лекція 3. РОЗВИТОК ЗАГАЛЬНОГО ПІДХОДУ ДО АНАЛІЗУ СТАНУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

План

1. Властивості сингулярних векторів блоку матриці цифрового зображення, що відповідають максимальному сингулярному числу
2. Зв'язок між нормованим вектором сингулярних чисел і сингулярнми векторами блоків оригінального цифрового зображення

1. Властивості сингулярних векторів блоку матриці цифрового зображення, що відповідають максимальному сингулярному числу

В якості інформаційної системи розглядається цифрове зображення (ЦЗ), формальним представленням якого є одна двовимірна матриця F.

На сьогоднішній день велике поширення отримала блокова обробка ЦЗ (блокова обробка матриць), яка використовується з різними цілями, коли обробці послідовно/паралельно піддаються окремі блоки, що отримуються в результаті розбивки матриці зображення. Така обробка використовується при збереженні ЦЗ в форматах з втратами (Jpeg, Jpeg2000), клонуванні, фотомонтажі, й не тільки. Найчастіше стеганоперетворення ЦЗ сучасними стеганографічними методами відбувається поблоково. Це пов’язано з декількома причинами:

1. Сучасні стеганографічні методи, як правило, повинні бути стійкими до стиску з втратами для забезпечення можливості збереження ЦЗ-стеганоповідомлення в такому форматі (Jpeg), що, крім іншого, дає можливість уникнути залучення додаткової уваги до отриманого зображення, у чому очевидно зацікавлені організатори прихованого каналу зв’язку. Оскільки алгоритм стиску Jpeg розбиває матрицю на блоки з наступною їх окремою обробкою, то для забезпечення можливості ефективного декодування вбудованої інформації після стиску стеганоповідомлення процес стеганоперетворення доцільно проводити також поблоково, керуючи складовими блока таким чином, щоб усунути можливість руйнування вбудованої інформації в результаті стиску, що й приводить до блокової обробки ЦЗ при вбудові додаткової інформації;
2. Сучасні стеганографічні методи повинні мати малу обчислювальну складність. Ця вимога стає критичною при необхідності забезпечення можливості їх роботи в режимі реального часу з потоковим контейнером, який усе частіше використовується на практиці. Обчислювальна складність будь-якого стеганографічного алгоритму, що здійснює блокове стеганоперетворення, буде визначатися кількістю блоків, тобто для $n \times n$-матриці F ЦЗ-контейнера складе $\underline{O}\left(n^2\right)$ операцій, що робить такий алгоритм перспективним для використання в умовах потокового контейнера;
3. Блокова обробка зображення, частковим випадком якої є стеганоперетворення, дає можливість легко розпаралелити цей процес, зокрема процес вбудови додаткової інформації, проводячи одночасно обробку декількох блоків, що для стеганоалгоритму забезпечує його перевагу в умовах потокового контейнера.

З врахуванням вище наведеного блокова обробка ЦЗ є розповсюдженою й широко використовуваною на сьогоднішній день.

Розіб’ємо F на квадратні непересічні $l \times l$-блоки B. Нехай

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

- нормальне сингулярне ррозкладання B, стовпці $u_1, \ldots, u_l$ матриці U і $v_1, \ldots, v_l$ матриці V – відповідно ліві і праві СНВ B, $\Sigma = diag\left(\sigma_1, \ldots, \sigma_l\right)$, $\sigma_1 \geq \ldots \geq \sigma_l \geq 0$ - СНЧ B.

СНВ u_1 и v_1, що відповідають максимальному СНЧ σ_1 блока B матриці ЦЗ, отримані в (3.1), є не тільки нечутливими до збурних дій в класичному сенсі (див. Методичні вказівки (частина 1) до виконання лабораторних робіт з дисципліни «Проблеми кібербезпеки та сучасні підходи до їх вирішення» для здобувачів другого (магістерського) рівня вищої освіти специальності 125 - Кібербезпека), а також sign-нечутливими, тобто такими, для яких при збурних діях не змінюються знаки їх компонент, близькими до n-оптимального вектору n^O простору R^l, де

$$n^O = \left(1/\sqrt{l}, 1/\sqrt{l}, \ldots, 1/\sqrt{l}\right)^T \in R^l$$

(для прикладу, n-оптимальний вектор простору R^2 - це бісектриса першого координатного кута координатної площини). Основою для цього висновку є теорема Фробеніуса.

По теоремі Фробеніуса будь-яка нерозкладна (див. нижче визначення поняття нерозкладнї матриці) невід'ємна матриця (тобто така матриця, усі елементи якої мають невід'ємні значення) M завжди має додатне власне значення $\bar{\lambda}(M)$, що є простим коренем характеристичного рівняння, таке, що модулі всіх інших власних значень не перевищують $\bar{\lambda}(M)$. Власному значенню $\bar{\lambda}(M)$ відповідає власний вектор $\bar{\varphi}(M)$ з додатними координатами.

Для матриці B матриця BB^T є симетричною невід'ємною матрицею, для якої має місце співвідношення (див.п.4 лекції 1-2):

$$BB^T = \left(U\Sigma V^T\right)\left(U\Sigma V^T\right)^T = U\Sigma^2 U^T,$$

яке в силу ортогональності матриці U і лексикографічної додатності її стовпців, а також діагональності матриці Σ^2 являє собою нормальне спектральне розкладання BB^T, що визначається однозначно (яке одночасно є й нормальним сингулярним розкладанням), при цьому власні значення матриці BB^T (які одночасно є її сингулярними числами) дорівнюють квадратам СНЧ B, зокрема, $\bar{\lambda}(BB^T) = \sigma_1^2(B)$, а ліві СНВ B - ортонормовані лексикографічно додатні власні вектори BB^T (які є одночасно і її лівими й правими СНВ). За теоремою Фробеніуса власному значенню $\bar{\lambda}(BB^T)$ відповідає власний вектор $\bar{\varphi}(BB^T)$ з додатними координатами, який є одночасно лівим СНВ u_1, що відповідає максимальному СНЧ σ_1 блока B. Тобто за теоремою Фробеніуса (при неразкладеності матриці BB^T) СНВ u_1, що відповідає максимальному СНЧ σ_1 блока B, має всі додатні координати (в випадку своєї лексикографічної додатності).

Аналогічне твердження буде випливати для правого СНВ v_1 блока B (див.п.4 лекції 1-2), що відповідає σ_1, оскільки для симетричної матриці $B^T B$ має місце рівність:

$$B^T B = \left(U\Sigma V^T\right)^T \left(U\Sigma V^T\right) = V\Sigma^2 V^T.$$

Таким чином, у будь-якій нерозкладній невід'ємній матриці, якою і є BB^T ($B^T B$), як буде показано нижче, лівий і правий СНВ, що відповідають максимальному СНЧ блоку B, мають додатні координати. Необхідно відзначити, що лівий (правий) СНВ, усі компоненти

якого додатні, що визначається нормальним сингулярним розкладанням, єдиний для B в силу ортонормованості СНВ. Важливо, що незалежно від збурної дії, якій піддається ЦЗ, матриці його блоків залишаються нерозкладними невід'ємними, а тому і обговорювані СНВ повинні після збурення (навіть сильного) мати всі додатні координати, тобто при будь-якій збурній дії залишитися в границях першого координатного ортанта (цей координатний ортант відповідає векторам (точкам), усі координати яких невід'ємні), тому ці вектори є не тільки нечутливими (стійкими), але й sign-нечутливими до будь-якої збурної дії (не змінюють знаків своїх компонентів при будь-якій збурній дії), причому ця властивість їм притаманна як до, та й після збурної дії, яка залишає матрицю BB^T нерозкладною невід'ємною. Очевидно, що це можливо лише в тому випадку, коли обговорювані СНВ будуть близькі до n-оптимального вектору n^O.

Покажемо, що BB^T є нерозкладною, тобто симетричними перестановками рядків і стовпців її не можна привести до виду:

$$\begin{pmatrix} A_1 & 0 \\ A_3 & A_2 \end{pmatrix}, \qquad (3.2)$$

де A_1, A_2 - $l_1 \times l_1$ і $l_2 \times l_2$-матриці відповідно, а 0 в матриці (3.2) позначає нульову матрицю розміром $l_1 \times l_2$.

Симетричні перестановки (якщо переставили і-ий і j-ий стовпці, то обов'язково переставляються і-ий й j-ий рядки й навпаки) в матриці можна одержати, використовуючи елементарні матричні операції й матриці перестановок: P - $l \times l$ – матриця перестановок (в кожному рядку і в кожному стовпчику P один елемент дорівнює одиниці, а всі інші – нулі). Матриця перестановок виходить із одиничної матриці шляхом перестановки тих рядків (стовпців) які ми прагнемо переставити у вхідній матриці. Якщо потрібно поміняти місцями рядки, то на отриману матрицю перестановки вхідна матриця множиться зліва, а якщо стовпці, то зправа.

Наприклад, нехай в матриці $W = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ треба переставити другий і третій рядки. Беремо одиничну матрицю відповідного розміру і в ній міняємо місцями другий і третій рядки:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Одержали потрібну матрицю перестановки P. При множенні на неї зліва матриці W, отримаємо:

$$PW = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 4 & 5 & 6 \end{pmatrix},$$

тобто в результуючій матриці помінялися місцями 2-ий і 3-ій рядки.

При множенні на P зправа поміняються місцями 2-ий і 3-ій стовпці:

$$WP = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 4 & 6 & 5 \\ 7 & 9 & 8 \end{pmatrix}.$$

У зв'язку з цим, результат симетричних перестановок (3.2) можна представити в матричному виді в такий спосіб:

$$\begin{pmatrix} A_1 & 0 \\ A_3 & A_2 \end{pmatrix} = PBB^T P^T$$

Враховуючи, що BB^T - симетрична, представлення (3.2) можна уточнити:

$$PBB^T P^T = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

(3.3)

де $A_1 = A_1^T$, $A_2 = A_2^T$.

Для того, щоб представлення (3.3) принципово було можливо, матриця BB^T повинна містити нульові елементи, причому цих елементів не може бути менше певного кількості, що залежить від розміру B, щоб вони могли сформувати нульові блоки в матриці $PBB^T P^T$ (3.3). Так для блоку 4×4 для розкладеності BB^T вона повинна містити не менше шести нульових значень (рис.3.1).

Елементи матриці BB^T виходять у результаті скалярного добутку рядків B. З урахуванням невід'ємності B нульове значення в BB^T можливо лише при наявності в B рядків, для яких кожна пара елементів, що належать одному стовпцю, обов'язково містила хоча б одне нульове значення. Для забезпечення шести нулів в BB^T таких пар рядків повинно бути три. Необхідне розташування елементів у рядках у блоці оригінального ЦЗ малоймовірно, причому ймовірність очевидно буде зменшуватися з зростанням розміру блоку, оскільки буде збільшуватися кількість потрібних для забезпечення виду (3.3) нулів в BB^T (наприклад, для $8 \times 8-$ блоку ця кількість повинна бути більше 13).

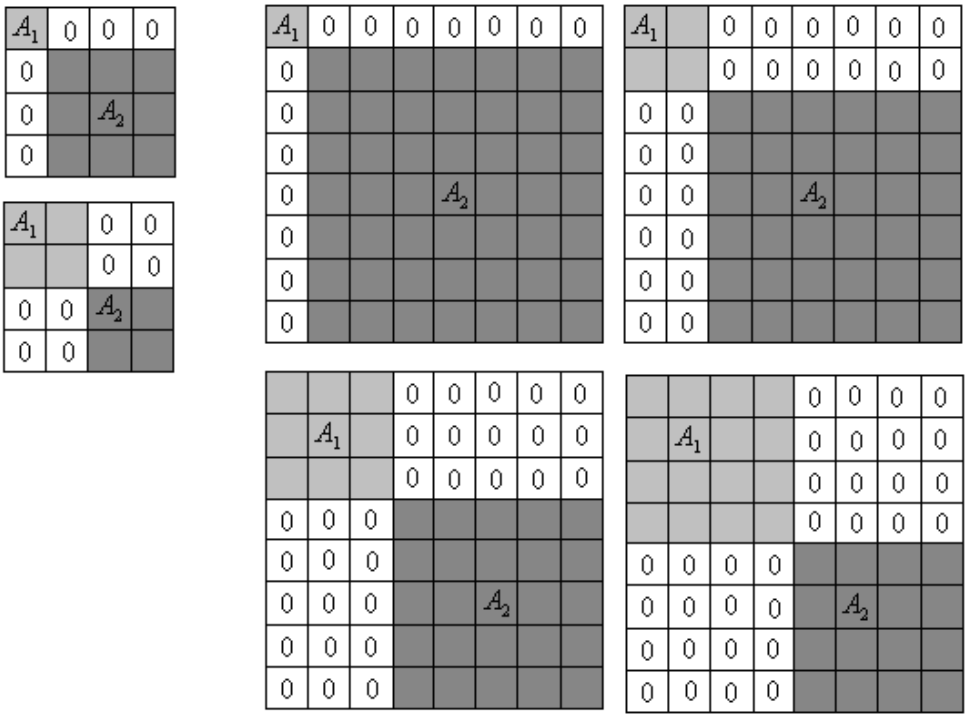


Рис.3.1. Можливий блочний вигляд матриці PBB^TP^T

Отримані висновки підтверджуються на практиці. Розглянемо ці блоки докладно.

Припустимо, що для BB^T можливо її представлення у вигляді (3.3) для деякої матриці перестановок $P=\overline{P}$. Матрицю $\overline{P}B\overline{P}^T$ розіб'ємо на підматриці $B_i, i=\overline{1,4}$: $\overline{P}B\overline{P}^T=\begin{pmatrix}B_1 & B_4\\ B_3 & B_2\end{pmatrix}$, де B_1, B_2 мають розміри $l_1\times l_1$ і $l_2\times l_2$ відповідно. Для B можливі два варіанти: $B_4=0$ (в цьому випадку B буде розкладною) і $B_4\neq 0$. Нехай $B_4=0$. Тоді:

$$\overline{P}BB^T\overline{P}^T=\overline{P}B\overline{P}^T\overline{P}B^T\overline{P}^T=\left(\overline{P}B\overline{P}^T\right)\left(\overline{P}B\overline{P}^T\right)^T=\begin{pmatrix}B_1 & 0\\ B_3 & B_2\end{pmatrix}\begin{pmatrix}B_1^T & B_3^T\\ 0 & B_2^T\end{pmatrix}=\begin{pmatrix}B_1B_1^T & B_1B_3^T\\ B_3B_1^T & B_3B_3^T+B_2B_2^T\end{pmatrix}. \quad (3.4)$$

Рівність $B_1B_3^T=0$ (відповідно до (3.3)) приведе до блокової діагональності матриці $\overline{P}BB^T\overline{P}^T$, у силу чого її спектр буде дорівнювати об'єднанню спектрів її блоків: матриць $B_1B_1^T$ і $B_3B_3^T+B_2B_2^T$. Таким чином, квадрати СНЧ B будуть визначати власні значення $B_1B_1^T$ і $B_3B_3^T+B_2B_2^T$. Рівність $B_1B_3^T=0$ з урахуванням невід'ємності матриць B_1 і B_3 можливо тоді, коли виконується наступна умова: кожному ненульовому елементу матриці B_1, що знаходиться в $k-$му стовпці, повинен відповідати нульовий $k-$й стовпець матриці B_3; в матриці B_3 $j-$й стовпець може бути ненульовим тільки, якщо нульовим буде $j-$й стовпець матриці B_1. Нульовий стовпець B_1 приведе к її виродженості, а також к виродженості $B_1B_1^T$, в силу чого спектр $B_1B_1^T$ буде містити нульове власне значення, а серед СНЧ B виявиться нульове, що, як показують численні обчислювальні експерименти, для оригінальних ЦЗ вкрай рідко, а у випадку ЦЗ у форматі без втрат практично неможливо.

Нехай $B_4\neq 0$. Тоді:

$$\overline{P}BB^T\overline{P}^T=\begin{pmatrix}B_1 & B_4\\ B_3 & B_2\end{pmatrix}\begin{pmatrix}B_1^T & B_3^T\\ B_4^T & B_2^T\end{pmatrix}=\begin{pmatrix}B_1B_1^T+B_4B_4^T & B_1B_3^T+B_4B_2^T\\ B_3B_1^T+B_2B_4^T & B_3B_3^T+B_2B_2^T\end{pmatrix}.$$

(3.5)

Матриця $\overline{P}BB^T\overline{P}^T$ (3.5) має вид (3.3) при

$$B_1B_3^T+B_4B_2^T=0 \quad\Leftrightarrow\quad \begin{cases}B_1B_3^T=0,\\ B_4B_2^T=0.\end{cases}$$

(3.6)

З урахуванням невід'ємності матриць $B_1,\ B_2,\ B_3,\ B_4$ і обговорюваного вище для виконання матричної рівності $B_1B_3^T=0$, задоволення системі (3.6) є вкрай малоймовірним.

Усі проведені вище міркування мають місце для квадратного блоку B будь-якого розміру.

Таким чином, на практиці можна вважати, що матриця BB^T для блоків оригінального ЦЗ (цифрового контенту) є нерозкладною. Тоді по теоремі Фробеніуса власному значенню $\overline{\lambda}(BB^T)$ відповідає власний вектор $\overline{\varphi}(BB^T)$ з додатними координатами, який є одночасно лівим СНВ u_1, що відповідає максимальному СНЧ σ_1 блока B.

Аналогічне твердження буде випливати для правого СНВ v_1 блока B (при розгляді замість BB^T матриці B^TB), що відповідає σ_1.

Таким чином, в матриці блока B лівий і правий СНВ, що відповідають максимальному СНЧ, мають додатні координати. Незалежно від збурної дії, матриці BB^T, B^TB будуть задовольняти (3.4) або (3.5), тобто залишаться невід'ємними нерозкладними, а тому і обговорювані СНВ після збурення будуть мати всі додатні координати, тому ці вектори є не тільки нечутливими, але й sign-нечутливими до будь-якої збурної дії. Це можливо лише в тому випадку, коли обговорювані СНВ близькі до n-оптимального вектору $n^O\in R^l$.

2. Зв'язок між нормованим вектором сингулярних чисел і сингулярними векторами блоків оригінального цифрового зображення

Представимо сингулярний спектр блока B в виді вектора $\sigma=(\sigma_1,\sigma_2,\ldots,\sigma_l)^T$ з простору R^l і нормуємо його:

$$\overline{\sigma}=\sigma/\|\sigma\|,$$

де – $\|\sigma\|$ норма вектора σ.

Вектор $\overline{\sigma}$ знаходиться в першому координатному ортанті R^l разом з лівим u_1 і правим v_1 СНВ, які відповідають σ_1. Незалежно від збурних дій всі СНЧ залишаються невід'ємними, до того ж в оригінальних ЦЗ хоча б одно з них (σ_1) буде додатним, що говорить про те, що вектор $\overline{\sigma}$ ніколи не змінить координатний ортант, в якому розташований, тобто є sign-нечутливим.

Таким чином, вектори u_1, v_1, $\bar{\sigma}$ мають спільні властивості, до того ж це має місце незалежно від конкретного виду формата ЦЗ:

- вони стійкі (нечутливі),
- sign-нечутливі,
- невід'ємні, розташовуються в першому координатному ортанті простору R^l.

Установлена спільність дає можливість припустити існування певного зв'язку між u_1, v_1, $\bar{\sigma}$ в блоках оригінального ЦЗ.

Елементи вектора $\bar{\sigma}$ мають характерні риси для блоків оригінального ЦЗ. Як показують численні обчислювальні експерименти,

$$\sigma_1 >> \sigma_i,\ i = 2,3,\ldots l. \qquad (3.7)$$

Ілюстрацією цьому є результати, наведені в табл.3.1 для $8\times 8-$блоків, для значень відокремленостей СНЧ.

Враховуючи (3.7), можна стверджувати, що перший компонент нормованого вектора СНЧ $\bar{\sigma}$ близький до 1, а інші компоненти $\bar{\sigma}$ близькі до 0. Наслідком цього є те, що кут між вектором $\bar{\sigma}$ і додатним напрямком координатної осі Ox_1 простору R^l у більшості блоків ЦЗ буде близький до нуля. Таким чином для блоку оригінального ЦЗ:

$$\angle(u_1,\bar{\sigma}) \approx \angle(v_1,\bar{\sigma}) \approx \angle(n^O,e_1). \qquad (3.8)$$

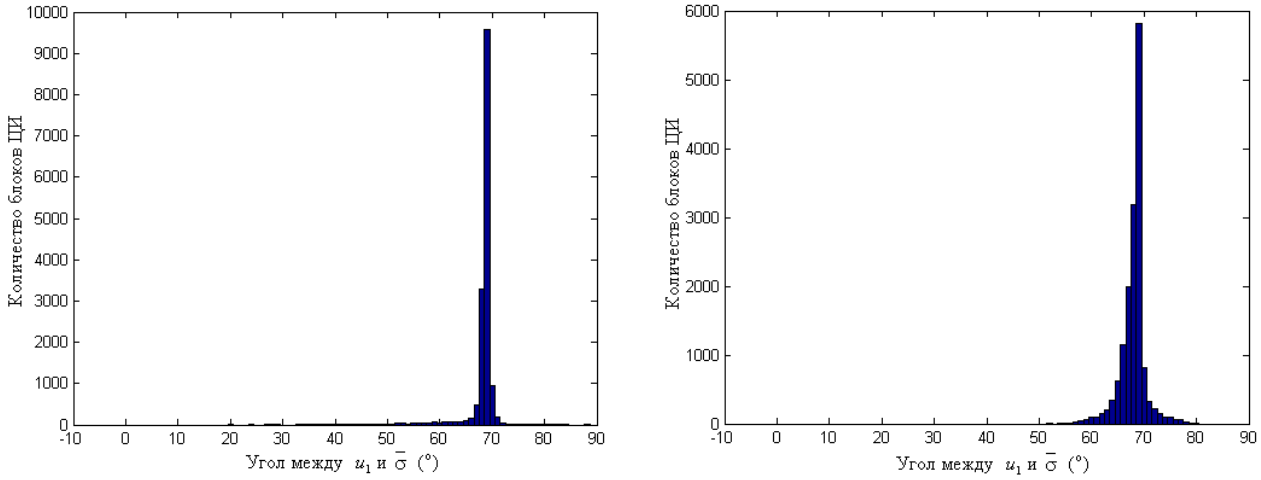
де $\angle(u_1,\bar{\sigma})$, $\angle(v_1,\bar{\sigma})$, $\angle(n^O,e_1)$ - кути між векторами u_1 і $\bar{\sigma}$, v_1 і $\bar{\sigma}$, n^O і вектором стандартного базису $e_1 = (1,0,\ldots,0)$ простору R^l, що відповідає додатному напряму осі Ox_1, відповідно.

Таблиця 3.1 – Середні значення відокремленості сингулярних чисел 8×8-блоків по 500 ЦЗ

Середнє значення $svdgap(i,B)$							
$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$
712.4564	23.1111	7.9843	3.0004	1.4232	0.7125	0.4667	0.5781

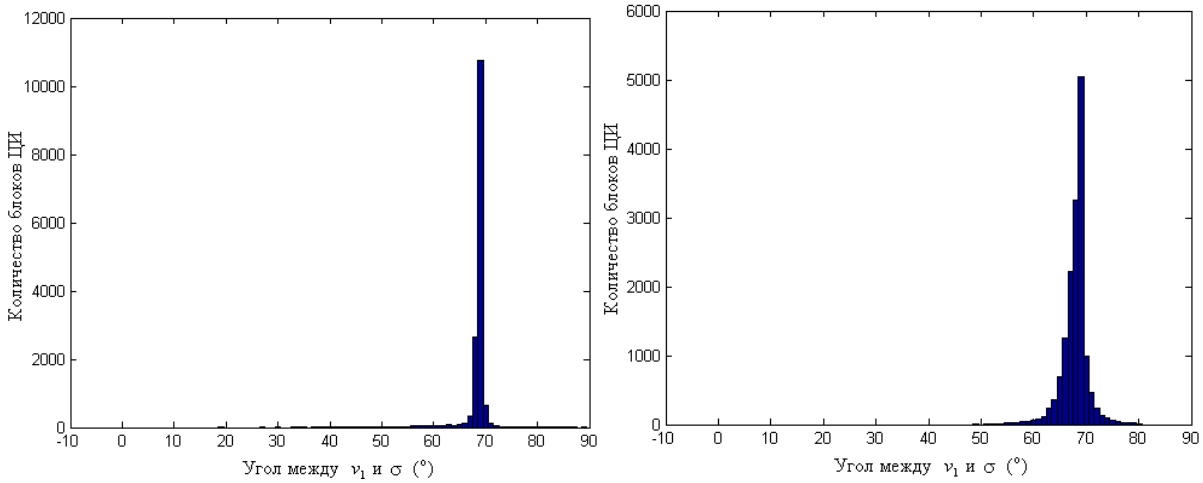
Для просторів R^4, R^8, R^{16}, R^{32} у градусному виразі наближені значення $\angle(n^O,e_1)$ відповідно визначаються $60.0°$, $69.5°$, $75.6°$, $79.9°$, даючи наближені значення кутів $\angle(u_1,\bar{\sigma})$, $\angle(v_1,\bar{\sigma})$ для більшості $l\times l-$блоків оригінального ЦЗ при конкретних значеннях l, що повністю підтверджується на практиці. Типові результати дослідження двох ЦЗ, одне з яких зберігалося у форматі JPEG, а інше в TIF, у вигляді гістограм (із кроком 1о) величин кутів між векторами u_1 і $\bar{\sigma}$ (ГU), блоків, отриманих у результаті стандартної розбивки ($l=8$) матриці зображення, представлені на рис.3.2. Аналогічним чином виглядають гістограми величин кутів між векторами v_1 і $\bar{\sigma}$ (ГV) (рис.3.3). Глобальний максимум (мода) гістограм у всіх випадках досягається для кута 70о, що, як підтверджують результати, наведені на рис.3.4, є невипадковим і відповідає (3.8). Рис.3.4 відбиває частоту появи конкретних значень кутів між аналізованими векторами, у яких досягається глобальний максимум ГU, ГV, що відповідають конкретним зображенням. Як видно, для більшості

протестованих ЦЗ максимум GU, GV досягається для кута 70о, причому для оригінальних ЦЗ, як і передбачалося, це ніяк не залежить від формату зберігання зображення.



а б

Рис. 3.2. Приклад гістограм значень кутів між векторами u_1 і $\bar{\sigma}$ 8×8-блоків в оригінальних ЦЗ: а – ЦЗ в форматі JPEG; б – ЦЗ в форматі TIF



а б

Рис.3.3. Приклад гістограм значень кутів між векторами v_1 і $\bar{\sigma}$ 8×8-блоків в оригінальних ЦЗ: а – ЦЗ в форматі JPEG; б – ЦЗ в форматі TIF

Питання

1. Властивості сингулярних векторів матриці, що відповідають максимальному сингулярному числу. Що означає sign-нечутливість вектора?
2. Поняття нерозкладної матриці.
3. Зв'язок між нормованим вектором сингулярних чисел і сингулярнми векторами блоків оригінального цифрового зображення.
4. Зв'язок між нормованим вектором сингулярних чисел і сингулярнми векторами блоків неоригінального цифрового зображення.
5. Показати, що кут між векторами u_1 і $\bar{\sigma}$, v_1 і $\bar{\sigma}$ для більшості $l\times l-$блоків оригінального цифрового зображення порівнянний з кутом між n-оптимальним вектором n^O и першим вектором стандартного базису простору R^l незалежно від формату зображення.

Література.

1. Гантмахер Ф.Р. Теория матриц: монография. 5-е изд. М.: Физматлит, 2004. 559 с. http://lib.brsu.by/sites/default/files/books/%D0%93%D0%B0%D0%BD%D1%82%D0%BC%D0%B0%D1%85%D0%B5%D1%80%20%D0%A4.%D0%A0.%20-%20%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F%20%D0%BC%D0%B0%D1%82%D1%80%D0%B8%D1%86.pdf
2. Кобозева А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. Праці Одеського політехнічного університету. 2014. 2. С. 136–146.
3. Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. Transport and Telecommunication Journal. 2016. 17(2). P. 128–137. http://dspace.opu.ua/jspui/bitstream/123456789/4003/1/Bobok_ttj-2016-0012.pdf
4. Бобок І.І Розвиток загального підходу до проблеми виявлення порушень цілісності цифрових зображень. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2017. 2(34). С. 78–88.
5. Хорошко В.О., Бобок І.І. Аналіз особливостей удосконаленого загального підходу до проблеми виявлення порушень цілісності цифрових зображень. Сучасна спеціальна техніка. 2019. 2(57). С. 59–71.

Лекція 4. РОЗВИТОК ЗАГАЛЬНОГО ПІДХОДУ ДО АНАЛІЗУ СТАНУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ (продовження)

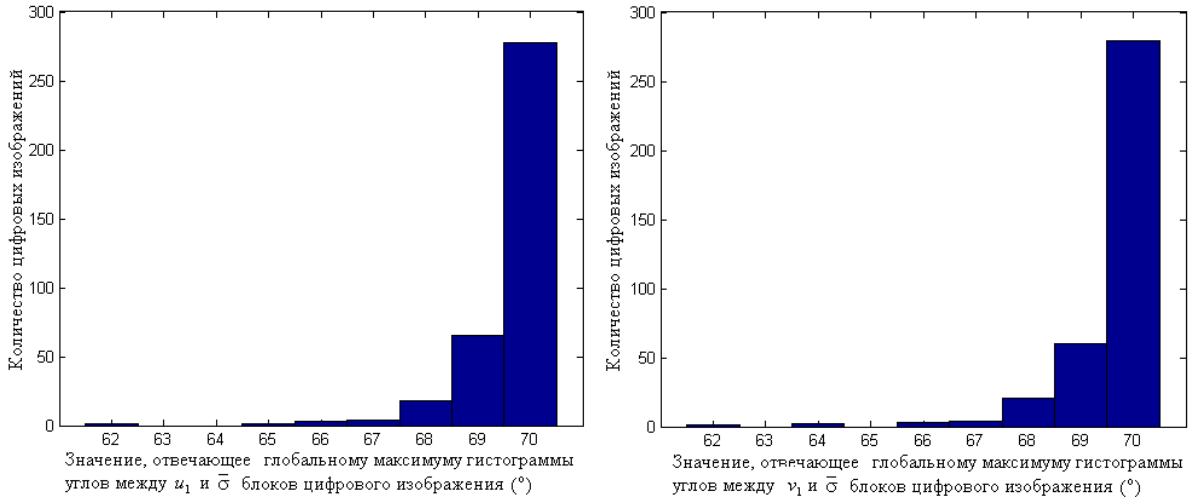
План

1. Вибір розміру блока
2. Особливості загального підходу для оригінальних і неоригінальних цифрових зображень

1. Вибір розміру блока

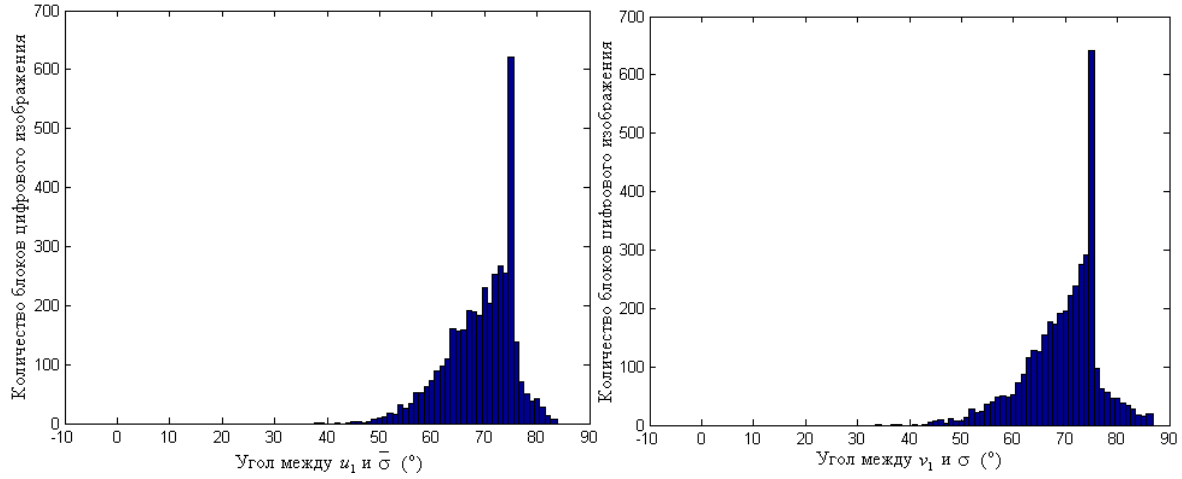
На перший погляд, у світлі нового підходу при аналізі ЦЗ має сенс використовувати блоки, по можливості, більшого розміру. Дійсно, якщо говорити, наприклад, про один з найпоширеніших у даний момент стеганометодів - методі модифікації найменшого значущого біта, то з урахуванням специфіки вбудови додаткової інформації (деякі елементи матриці контейнера можуть не змінити свого значення, якщо останній значущий біт використовуваного для вбудови пікселя збігається із черговим бітом, що вбудовується) при малій пропускній спроможності прихованого каналу звязку і малому розмірі блоку, що використовується для аналізу ЦЗ, порушення встановлених співвідношень між визначальними формальними параметрами в стеганоповідомленні в порівнянні з контейнером буде вкрай складно виявити. Співвідношення (3.8) перевірялось в ході обчислювального експерименту для $l \times l -$блоків, де $l = 16$ (рис.3.5,3.6) і $l = 32$ (рис.3.7). Результати експерименту в цілому відповідати (3.8), однак характер гістограм ГU, ГV «погіршується»: хоча глобальний максимум і відповідає (3.8), кількість блоків, у яких кут відрізняється від очікуваного значення, збільшується в порівнянні з картиною для блоків розміру 8×8.

Отримані результати змушують відмовитися при аналізі ЦЗ від блоків, для яких $l > 8$. Очевидно, що співвідношення (3.8) будуть тим точніше виконуватися, чим менше буде l. Підтвердженням є результати обчислювального експерименту для $4 \times 4 -$блоків (рис.3.8). Глобальний максимум ГU, ГV тут досягається в значеннях: 58о – 0.8% від загальної кількості ЦЗ, задіяних в експерименті, 59о – 0.8% , 60о – 82%, 61о – 17% від загальної кількості ЦЗ, задіяних в експерименті. Це робить $4 \times 4 -$блоки такими, яким надається перевага при аналізі ЦЗ, заснованому на співвідношенні (3.8).



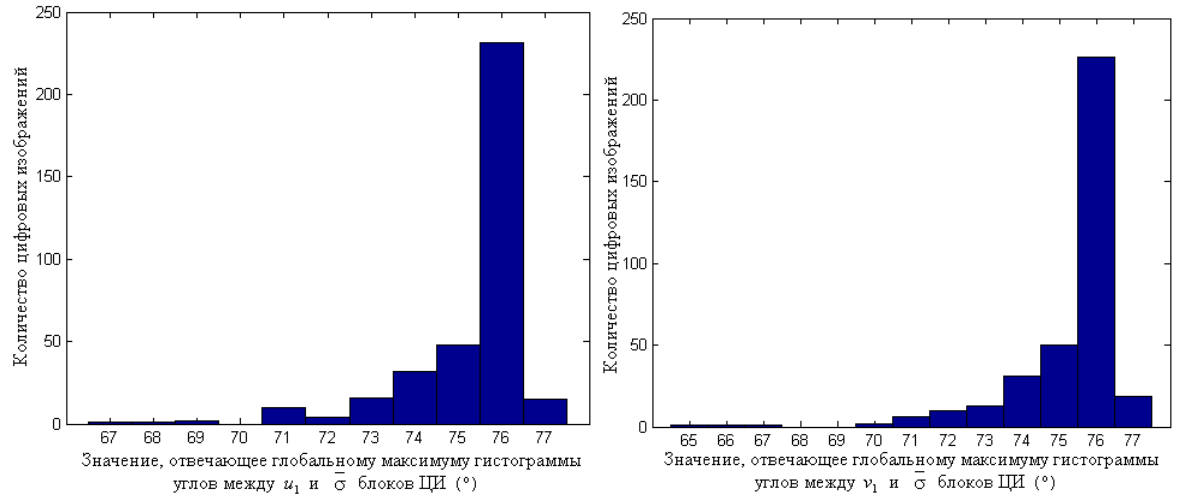
а б

Рис.3.4. Гістограми значень мод ГU (а), ГV (б) 8×8-блоків матриць ЦЗ



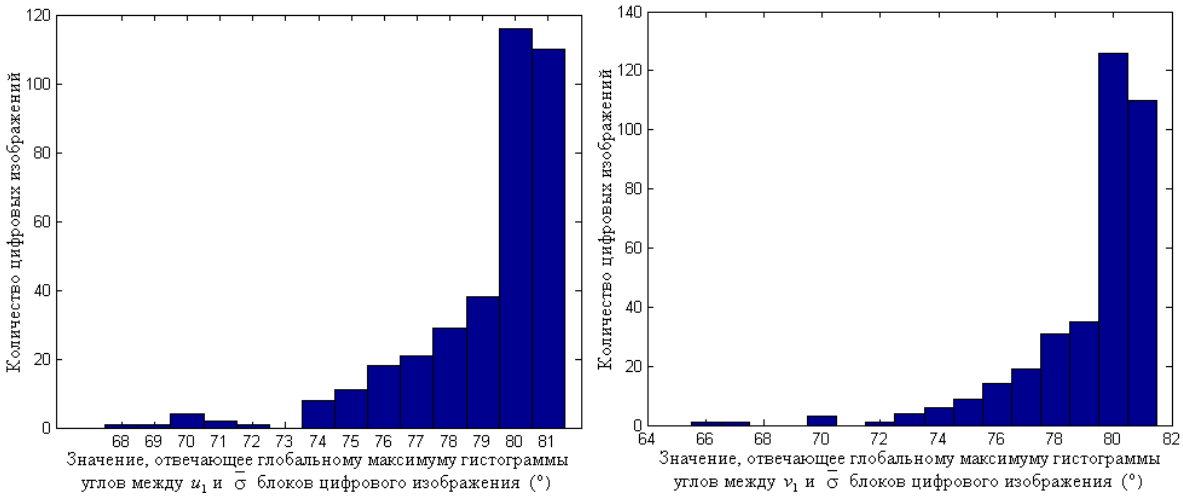
а б

Рис.3.5. Приклад гістограм значень кутів між векторами u_1 і $\bar{\sigma}$ (а), v_1 і $\bar{\sigma}$ (б) 16×16-блоків матриць оригінальних ЦЗ



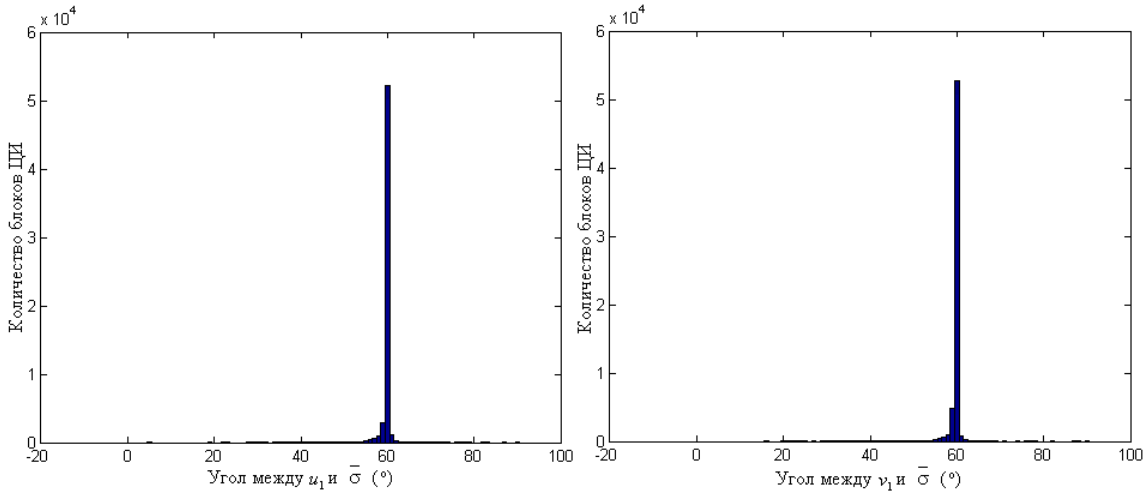
а б

Рис.3.6. Гістограми значень мод гістограм значень кутів між векторами u_1 і $\bar{\sigma}$ (а), v_1 і $\bar{\sigma}$ (б) 16×16-блоків матриць цифрових зображень



а б

Рис.3.7. Гістограми значень мод гистограм значень кутів між векторами u_1 і $\bar{\sigma}$ (а), v_1 і $\bar{\sigma}$ (б) 32×32- блоків матриць цифрових зображень

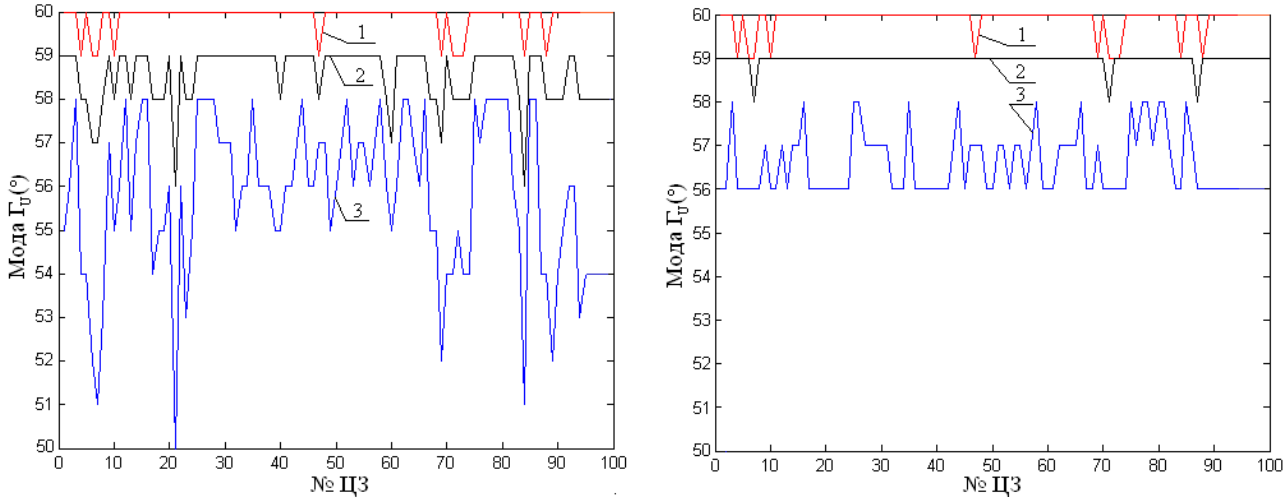


а б

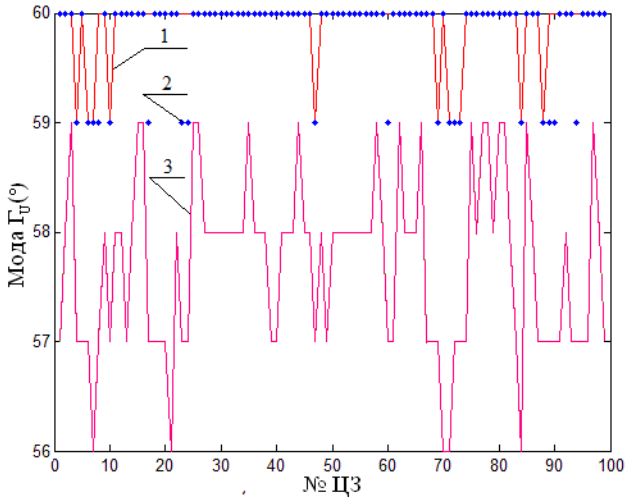
Рис.3.8. Приклад гістограм значень кутів між векторами u_1 і $\bar{\sigma}$ (а), v_1 і $\bar{\sigma}$ (б) 4×4-блоків в оригінальних ЦЗ

2. Особливості загального підходу для оригінальних і неоригінальних цифрових зображень

Установлені співвідношення (3.8) характерні для оригінальних ЦЗ. При збуренні ЦЗ ці співвідношення часто будуть порушуватися, що підтверджується на практиці (рис.3.9). У ході експерименту для оригінальних ЦЗ будувалися ГU, ГV, для яких визначався аргумент, у якому досягався глобальний максимум (мода гістограми) (крива 1 на рис.3.9), потім на ЦЗ накладався шум (аддитивний гауссовський з нульовим маточіуванням і дисперсією $D=0.001,\ 0.01$; мультиплікативний з дисперсиейією $D=0.001,\ 0.01$; шум «сіль-перець» з $d=0.05$, пуассонівський шум). Для збурених ЦЗ будувалися ГU, ГV (рис.3.9 криві 2 і 3 відповідно). Криві, що відповідають збуреним ЦЗ, певним чином відрізняються від кривих, відповідних до оригінальних зображень: значення аргументів глобальних максимумів ГU, ГV для зашумлених ЦЗ в переважній більшості менше, чим для оригінальних. Навіть у випадку, коли спостерігається збіг, як, наприклад, для ЦЗ №47 (рис.3.9(б)), для якого аргументи глобальних максимумів гістограм кутів між v_1 і $\bar{\sigma}$ для оригінального ЦЗ і зашумленого (гауссовський шум з $D=0.001$) дорівнюють 60, розрізнити оригінальне й збурене ЦЗ не складно (рис.3.10): значення глобального максимуму для оригінального ЦЗ в 2 рази більше, чим для збуреного; гістограма для зашумленого ЦЗ «ширше» гістограми для оригінального.



а б

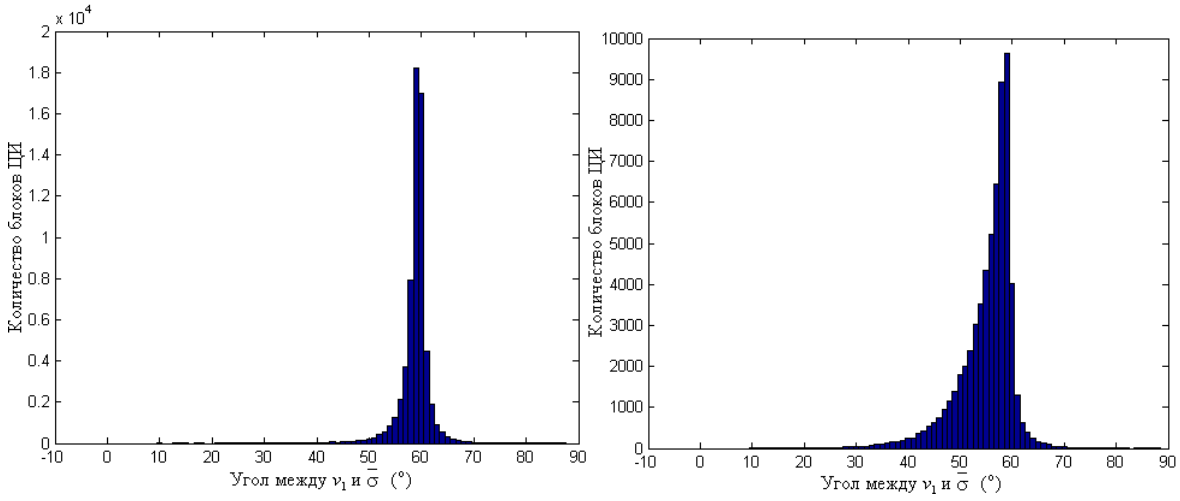


в

Рис. 3.9. Графіки відповідності моди ГU і номера ЦЗ: а –1 – оригінальне ЦЗ; 2 – зашумлене ЦЗ (гауссівський шум з нульовим математичним очікуванням і $D = 0.001$); 3 – зашумлене ЦЗ (гауссівський шум з нульовим математичним очікуванням і $D = 0.01$); б – 1 – оригінальне ЦЗ; 2 – зашумлене ЦЗ (мультиплікативний шум з $D = 0.001$); 3 – зашумлене ЦЗ (мультиплікативний шум з $D = 0.01$); в – 1 – оригінальне ЦЗ; 2 – зашумлене ЦЗ (шум «сіль-перець» з $d = 0.05$); 3 – зашумлене ЦЗ (пуассонівський шум)

Картина зі зменшенням значення глобального максимуму й «розширенням» гістограми для збуреного ЦЗ в порівнянні з оригінальним має місце й у випадку, коли аргумент гістограми, у якому цей глобальний максимум досягається, змінюється (зменшується) у зашумленому ЦЗ. Співвідношення між значенням глобального максимуму ГU, ГV і «шириною» гістограми, оціненою певним чином, є додатковою визначальною характеристикою, що дозволяє відокремлювати оригінальне ЦЗ від збуреного.

Таким чином, для збурених ЦЗ спостерігається порушення співвідношень (3.8) для більшості блоків зображення.



а

Рис.3.10. Гістограми конкретного оригінального (а) і зашумленого (гауссовський шум з нульовим маточікуванням і $D = 0.001$) (б) ЦЗ (блоки розміру 4×4)

Таким чином:

1. для більшості блоків оригінального ЦЗ незалежно від формату його зберігання (із втратами, без втрат) СНВ u_1, v_1, що відповідають максимальному СНЧ, а також нормований

вектор СНЧ $\overline{\sigma}$ мають загальні властивості: нечутливість (стійкість), sign-нечутливість до збурних дій, у тому числі, значних, невід'ємність;

2. кут між векторами u_1 і $\overline{\sigma}$, v_1 і $\overline{\sigma}$ для переважної більшості $l \times l -$блоків оригінального ЦЗ є близьким до кута між n-оптимальним вектором n^O і першим вектором стандартного базису простору R^l незалежно від формату ЦЗ;

3. для збурених ЦЗ співвідношення $\angle(u_1, \overline{\sigma}) \approx \angle(v_1, \overline{\sigma}) \approx \angle(n^O, e_1)$ буде порушуватися для більшості блоків, що є показником порушення цілісності ЦЗ.

Отримані результати можуть бути використані для розробки методів виявлення порушення цілісності ЦЗ.

Питання

1. Властивості сингулярних векторів матриці, що відповідають максимальному сингулярному числу. Що означає sign-нечутливість вектора?
2. Зв'язок між нормованим вектором сингулярних чисел і сингулярнми векторами блоків оригінального цифрового зображення.
3. Зв'язок між нормованим вектором сингулярних чисел і сингулярнми векторами блоків неоригінального цифрового зображення.
4. Показати, що кут між векторами u_1 і $\overline{\sigma}$, v_1 і $\overline{\sigma}$ для більшості $l \times l -$блоків оригінального цифрового зображення порівнянний з кутом між n-оптимальним вектором n^O и першим вектором стандартного базису простору R^l незалежно від формату зображення.
5. Які фактори враховувалися при виборі розміру блоку?
6. В чому полягають особливості загального підходу для оригінальних і неоригінальних цифрових зображень?

Література.

1. Гантмахер Ф.Р. Теория матриц: монография. 5-е изд. М.: Физматлит, 2004. 559 с. http://lib.brsu.by/sites/default/files/books/%D0%93%D0%B0%D0%BD%D1%82%D0%BC%D0%B0%D1%85%D0%B5%D1%80%20%D0%A4.%D0%A0.%20-%20%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F%20%D0%BC%D0%B0%D1%82%D1%80%D0%B8%D1%86.pdf
2. Кобозева А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. Праці Одеського політехнічного університету. 2014. 2. С. 136–146.
3. Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. Transport and Telecommunication Journal. 2016. 17(2). P. 128–137. http://dspace.opu.ua/jspui/bitstream/123456789/4003/1/Bobok_ttj-2016-0012.pdf
4. Бобок І.І Розвиток загального підходу до проблеми виявлення порушень цілісності цифрових зображень. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2017. 2(34). С. 78–88.
5. Хорошко В.О., Бобок І.І. Аналіз особливостей удосконаленого загального підходу до проблеми виявлення порушень цілісності цифрових зображень. Сучасна спеціальна техніка. 2019. 2(57). С. 59–71.

6. Лекція 5. АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАГАЛЬНОГО ПІДХОДУ ДО ПРОБЛЕМИ ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ У РІЗНИХ ФОРМАТАХ ЗБЕРЕЖЕННЯ
7. План

8. 1. Дослідження значення кута між $\overline{\sigma}$ і e_1 блоку зображення, збереженого з/без втрат для відповідних зображень.
9. 2. Дослідження значення кута між $\overline{\sigma}$ і e_1 блоку зображення, збереженого з/без втрат для невідповідних зображень.
10.
11. 1.Дослідження значення кута між $\overline{\sigma}$ і e_1 блоку зображення, збереженого з/без втрат для відповідних/невідповідних зображень.
12. Далі ЦЗ, що відрізняються тільки форматом їх збереження (з/без втрат), називаються відповідними.
13. Нехай B – $l \times l$-блок матриці ЦЗ після її стандартного розбиття, СНЧ якого – $\sigma_1,\ldots,\sigma_l$.
14. СНЧ блоків ЦЗ, збереженого в форматі без втрат (ФбВ), мають певні особливості в порівнянні з СНЧ ЦЗ в форматі з втратами (ФзВ). Оскільки стиск ЦЗ відбувається за рахунок квантування й наступного округлення частотних коефіцієнтів (в Jpeg – коефіцієнтів дискретного косинусного перетворення (ДКП)) блоків матриці, то це, за рахунок особливостей матриць квантування (див. рис. 5.1), приводить до зменшення внеску високочастотної й (можливо) середньочастотної складових у стисненому ЦЗ, у порівнянні з відповідним йому, але у ФбВ. Враховуючи зв'язок частотного й сингулярного спектрів матриці/блоку матриці, що відповідає ЦЗ, а саме, що сингулярні трійки з максимальними СНЧ відповідають, головним чином, низькочастотній складовій сигналу, а середньо- і високочастотним складовим відповідають, головним чином, сингулярні трійки з СНЧ, середніми й найменшими за значенням, то стиск ЦЗ у $l \times l$-блоці очевидно буде приводити до зменшення сукупного внеску $\sigma_2,\ldots,\sigma_l$, який виражається як $\sigma_2{}^2 + \ldots + \sigma_l{}^2$, відповідно до формули:

$$\sum_{u=0}^{l-1}\sum_{v=0}^{l-1} P(u,v) = \sum_{i=1}^{l} \sigma_i^2 , \qquad (5.1)$$

де $P(u,v), u = \overline{0,l-1}, v = \overline{0,l-1}$, — енергетичний спектр блоку B, в блоці стиснутого ЦЗ, у порівнянні з їхнім внеском у відповідному блоці відповідного ЦЗ в ФбВ, при цьому σ_1 змінюється незначно при збереженні в Jpeg з коефіцієнтами якості $QF \geq 65$, зокрема $QF \in \{65,75,85\}$, що найбільш часто використовуються на практиці. Для ілюстрації в табл. 5.1 наведені приклади сингулярних спектрів випадково обраних відповідних блоків у різних парах відповідних ЦЗ, які спочатку зберігалися у ФбВ, а потім були перезбережені в ФзВ (ФзВ – Jpeg з QF=75) для $l = 4$.

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

Рис.5.1. Приклад матриці квантування

Має місце наступна теорема.

Теорема. Якщо ЦЗ є відповідними, то співвідношення (3.8) (лекція 3-4) буде виконуватися з більшою точністю для блоків ЦЗ у ФзВ ніж для ЦЗ в ФбВ, що приведе при перезбереженні ЦЗ з ФбВ в ФзВ до збільшення кількості блоків, для яких $\angle\left(u_1,\overline{\sigma}\right)=\angle\left(n^O,e_1\right)$.

Доказ. Нехай B – $l\times l$-блок ЦЗ в ФбВ, нормований вектор СНЧ якого – $\overline{\sigma}$. Відповідний йому блок ЦЗ, перезбереженого в ФзВ, позначимо B^J. Відповідний B^J нормований вектор СНЧ позначимо $\overline{\sigma}^J$, СНЧ B^J: $\sigma_i^{\ J}, i=\overline{1,l}$. Тоді з урахуванням визначення скалярного добутку двох векторів і нормованості $\overline{\sigma}$, $\overline{\sigma}^J$, e_1:

$$\angle\left(e_1,\overline{\sigma}\right)=arccos\frac{\sigma_1}{\sqrt{\sigma_1^2+\ldots+\sigma_l^2}}, \qquad (5.2)$$

$$\angle\left(e_1,\overline{\sigma}^J\right)=arccos\frac{\sigma_1^{\ J}}{\sqrt{\left(\sigma_1^J\right)^2+\ldots+\left(\sigma_l^J\right)^2}}. \qquad (5.3)$$

З врахуванням того, що, як показано вище,

$$\left(\sigma_2^J\right)^2+\ldots+\left(\sigma_l^J\right)^2<\sigma_2^2+\ldots+\sigma_l^2, \text{ а } \sigma_1^J\approx\sigma_1,$$

маємо

$$\frac{\sigma_1^{\ J}}{\sqrt{\left(\sigma_1^J\right)^2+\ldots+\left(\sigma_l^J\right)^2}}>\frac{\sigma_1}{\sqrt{\left(\sigma_1\right)^2+\ldots+\left(\sigma_l\right)^2}},$$

тоді з (5.2), (5.3):

$$\angle\left(e_1,\overline{\sigma}^J\right)<\angle\left(e_1,\overline{\sigma}\right). \qquad (5.4)$$

Таким чином, враховуючи, що (3.8) було отримано, між іншим, на основі того, що кут між вектором $\overline{\sigma}$ і додатним напрямком координатної осі Ox_1 простору R^l у більшості блоків ЦЗ є близьким до нуля, очевидно, що за рахунок меншої відмінності в блоках ЦЗ у ФзВ ніж ЦЗ в ФбВ нормованого вектора СНЧ від вектора e_1, для відповідних ЦЗ співвідношення (3.8) буде виконуватися з більшою точністю для ЦЗ у ФзВ, тобто кути $\angle\left(u_1,\overline{\sigma}\right)$, $\angle\left(v_1,\overline{\sigma}\right)$ в ЦЗ в ФзВ будуть менше відрізнятися від $\angle\left(n^O,e_1\right)$, ніж у відповідному ЦЗ в ФбВ, а це приведе до того, що кількість блоків, для яких $\angle\left(u_1,\overline{\sigma}\right)=\angle\left(n^O,e_1\right)$, в відповідному ЦЗ в ФзВ буде більшою, що й потрібно було довести.

Таблиця 5.1

Сингулярні спектри відповідних 4×4-блоків відповідних ЦЗ в різних форматах збереження

ЦЗ	Блок ЦЗ в ФбВ	Відповідний блок ЦЗ в ФзВ

	Сингулярний спектр	$\sigma_2^2+\sigma_3^2+\sigma_4^2$	Сингулярний спектр	$\sigma_2^2+\sigma_3^2+\sigma_4^2$
1	992.7711, 1.4424, 0.6928, 0.0081	2.5606	992.0000, 0, 0, 0	0
2	732.2567, 3.8380, 0.8782, 0.2270	15.5530	733.2530, 1.0000, 0.6420, 0.3905	1.5647
3	206.0885, 9.6091, 1.7961, 0.9953	96.5514	204.0000, 0, 0, 0	0

З урахуванням специфіки організації процесу стиску можна стверджувати, що чим нижче буде коефіцієнт якості QF, тим менше буде сукупний енергетичний внесок другого і т.д., l-го СНЧ у відповідний блок малого розміру ЦЗ (відповідно до (5.1)), що приведе до зменшення кута між нормованим вектором СНЧ і вектором e_1 зі зменшенням QF, тобто при $i_1 \geq i_2$ буде мати місце співвідношення:

$$k \geq k_{(i_1)} \geq k_{(i_2)}, \qquad (5.5)$$

де k – середнє по блоках ЦЗ значення величини кута між нормованим вектором СНЧ і вектором e_1 в блоці для зображення в ФбВ; $k_{(i_1)}, k_{(i_2)}$ – кількісні показники, аналогічні k, але для відповідних ЦЗ в ФзВ з $QF = i_1$, $QF = i_2$ відповідно.

При проведенні обчислювального експерименту було задіяно 500 ЦЗ, спочатку збережених у форматі Tif, які в ході експерименту перезберігалися в Jpeg з $QF \in \{65,70,75,80,85,90\}$. Ця множина ЦЗ називається експериментальною (ЕМ). Розбивка матриці ЦЗ відбувалася на 4×4-блоки.

В результаті обчислювального експерименту отримано: для 98.7% цифрових зображень при перезбереженні їх з Tif в Jpeg було зафіксовано монотонне спадання середнього значення по блоках зображення кута між нормованим вектором СНЧ і вектором e_1 зі зменшенням значення QF:

$$k \geq k_{(90)} \geq k_{(85)} \geq k_{(80)} \geq k_{(75)} \geq k_{(70)} \geq k_{(65)}. \qquad (5.6)$$

В результаті обчислювального експерименту по всім ЦЗ з ЕМ було встановлено, що

$$k \in [0.239, 6.40],\ k_{(90)} \in [0.12, 4.56],\ k_{(85)} \in [0.09, 2.78],\ k_{(80)} \in [0.05, 2.71],$$

$$k_{(75)} \in [0.035, 2.56],\ k_{(70)} \in [0.025, 2.46],\ k_{(65)} \in [0.011, 2.32],$$

при цьому $k_{sr} = 1.87$, $k_{(90)_{sr}} = 1.12$, $k_{(85)_{sr}} = 1.01$, $k_{(80)_{sr}} = 0.941$, $k_{(75)_{sr}} = 0.907$, $k_{(70)_{sr}} = 0.856$, $k_{(65)_{sr}} = 0.818$, де k_{sr}, $k_{(i)_{sr}}$, $i \in \{65,70,75,80,85,90\}$ – середні значення k, $k_{(i)}$ по всім ЦЗ відповідно.

Таким чином:

$$k_{sr} > k_{(90)_{sr}} > k_{(85)_{sr}} > k_{(80)_{sr}} > k_{(75)_{sr}} > k_{(70)_{sr}} > k_{(65)_{sr}}.$$

Черговим практичним підтвердженням (5.4), (5.5) є систематичне незбільшення моди гістограми значень розглянутих кутів з одночасним збільшенням значення гістограми в моді при порівнянні цих гістограм для відповідних цифрових зображень в форматі Tif і Jpeg (із зменшенням коефіцієнту якості QF) (табл. 5.2). Типовий вид гістограм представлений на рис. 5.2.

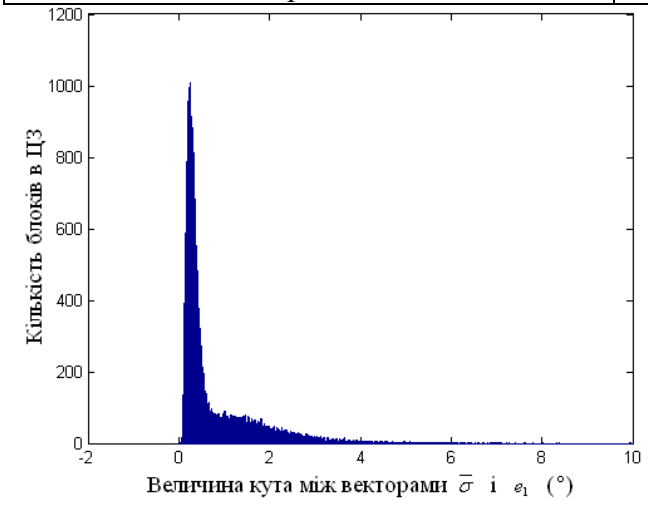
Таким чином, співвідношення (3.8) буде виконуватися точніше для оригінального ЦЗ у ФзВ, ніж для відповідного йому ЦЗ у ФбВ, у тому розумінні, що в блоці ЦЗ у ФзВ кут $\angle\left(u_1,\overline{\sigma}\right)$ ($\angle\left(v_1,\overline{\sigma}\right)$) буде ближче до $\angle\left(n^O,e_1\right)$, а тому блоків, для яких $\angle\left(u_1,\overline{\sigma}\right)=\angle\left(n^O,e_1\right)$, буде більше. Такий висновок знаходить підтвердження на практиці: у розглянутих ЦЗ з ЕМ у форматі Tif у середньому $\approx 32\%$ $4\times 4-$блоків мають $\angle\left(u_1,\overline{\sigma}\right)=60^o$, у той час, як для відповідних ЦЗ в Jpeg аналогічний параметр дорівнює $\approx 39.5\%$, $\approx 40.4\%$, $\approx 41.7\%$ для $QF\in\{85,75,65\}$ відповідно, збільшуючись, як і слід було очікувати, зі зменшенням значення коефіцієнта якості QF.

До сих пір в експериментах були задіяні відповідні цифрові зображення в різних (з/без втрат) форматах збереження. При проведенні обчислювального експерименту, у якому були задіяні 600 зображень у форматах з втратами і без втрат, що не були відповідними, а обиралися випадковим чином, при цьому зображення в форматі Jpeg мали різні коефіцієнти якості від 65 до 100, розглянутий кількісний параметр практично не відрізнявся для цифрових зображень в форматі з втратами і без втрат: $\approx 33.2\%$, $\approx 32.7\%$ блоків відповідно.

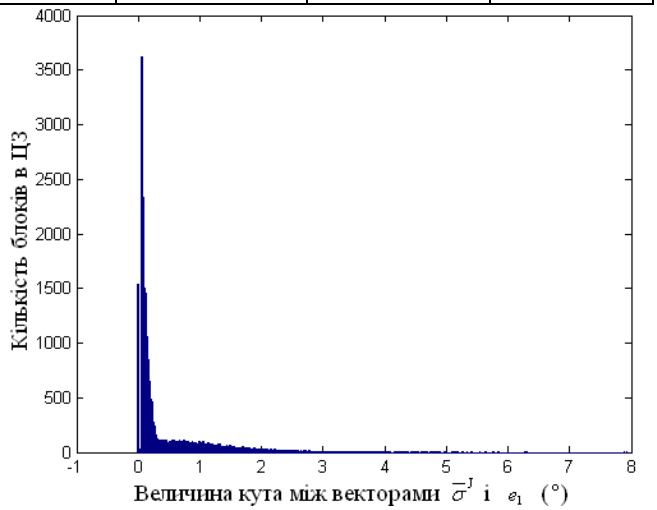
Таблиця 5.2

Характер зміни моди гістограми значень кутів між нормованим вектором сингулярних чисел і вектором e_1 в 4×4-блоках цифрового зображення з експериментальної множини при перезбереженні зображення з Tif в Jpeg з коефіцієнтом якості $QF\in\{65,75,85\}$

Значення моди гістограми (в градусах) (по ЦЗ з ЕМ)	Tif	$QF=85$	$QF=75$	$QF=65$
Мінімальне	0	0	0	0
Максимальне	4.67	1.45	1.06	1.14
Середнє	0.96	0.45	0.22	0.11



а



б

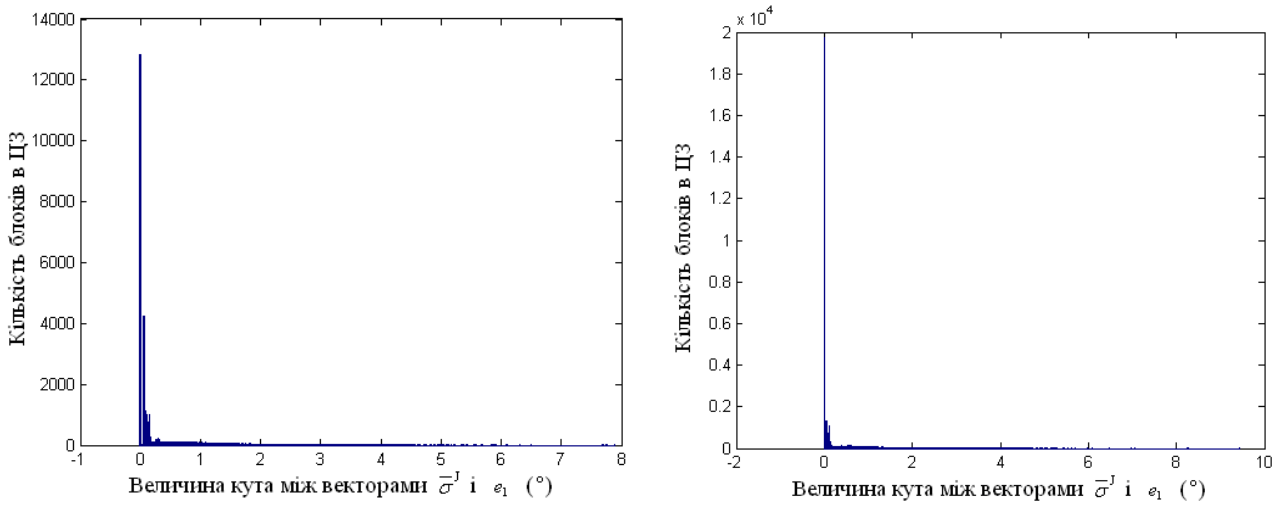


Рис. 5.2. Гістограми кутів між векторами $\bar{\sigma}$ ($\bar{\sigma}^J$) і e_1 4×4-блоків для: а – ЦЗ в форматі Tif (мода – 0.26 градуса, значення в моді – 1009 блоків; середнє значення кута по ЦЗ – 0.76 градуса); б – відповідне ЦЗ в форматі Jpeg (QF=85) (мода – 0.06 градуса, значення в моді – 3618 блоків; середнє значення кута – 0.46 градуса); в – відповідне ЦЗ в форматі Jpeg (QF=75) (мода – 0.0 градуса, значення в моді – 12837 блоків; середнє значення кута – 0.42 градуса); г – відповідне ЦЗ в форматі Jpeg (QF=65) (мода – 0.0 градуса, значення в моді –19744 блоків; середнє значення кута – 0.38 градуса).

Питання

1. Які зображення називаються відповідними?
2. Як співвідносяться кути між $\bar{\sigma}$ і e_1 блоку зображення, збереженого з/без втрат для відповідних/невідповідних зображень? Пояснити.

Література

1. Бобок І.І., Кобозєва А.А. Особливості нового підходу до вирішення проблеми виявлення порушень цілісності цифрових зображень в різних форматах збереження. Безпека інформації. 2017. 23(3). С. 197–203 https://core.ac.uk/download/pdf/296366114.pdf
2. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с. https://studizba.com/files/show/pdf/53191-1-dzh-demmel--vychislitel-naya-lineynaya.html
3. И.Бобок, «Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров»,Інформатика та математичні методи в моделюванні, Т.7, No3, С.211-219, 2017.

Лекція 6. АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАГАЛЬНОГО ПІДХОДУ ДО ПРОБЛЕМИ ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ У РІЗНИХ ФОРМАТАХ ЗБЕРЕЖЕННЯ (продовження)

План

1. Дослідження залежності чутливості вектору $\bar{\sigma}$ блоку від формату збереження цифрового зображення.

2. Дослідження залежності чутливості векторів u_1, v_1 блоку від формату збереження зображення.

1. Дослідження залежності чутливості вектору $\bar{\sigma}$ блоку від формату збереження цифрового зображення.

Ефективність та доцільність використання співвідношення (3.8) для відокремлення оригінального ЦЗ від такого, цілісність якого порушена, очевидно залежить від ступеня чутливості до ЗД формальних параметрів блоків ЦЗ, що там фігурують: нормованого вектора СНЧ та СНВ, що відповідають максимальному СНЧ.

В загальному випадку нормований вектор СНЧ будь-якої матриці М є нечутливим до ЗД, що очевидно витікає зі співвідношення, що має місце для СНЧ $\sigma_i(M)$ матриці М:

$$\max_i \left|\sigma_i(M) - \sigma_i(M + \Delta M)\right| \le \left\|\Delta M\right\|_2, \qquad (5.7)$$

де – ΔM матриця збурення М, $\|\bullet\|_2$ — спектральна матрична норма, але кількісно ця нечутливість для ЦЗ в різних форматах може відрізнятися.

З'ясуємо, як формати відповідних ЦЗ впливають на чутливість нормованого вектора СНЧ блоку.

Теорема. Якщо ЦЗ є відповідними, то чутливість нормованого вектора СНЧ блоку до ЗД, що відрізняються від стиску з втратами, більше для ЦЗ у ФзВ; чутливість буде зростати зі зменшенням коефіцієнту якості, що використовувався при отриманні відповідного ЦЗ у ФзВ.

Доказ. Нехай координати нормованого вектора СНЧ $\bar{\sigma}$ $l \times l$-блоку В ЦЗ в ФбВ – $\bar{\sigma}_i, i = \overline{1,l}$, координати нормованого вектора СНЧ $\bar{\sigma}^J$ відповідного йому блоку B^J ЦЗ, перезбереженого в ФзВ, $\bar{\sigma}_i{}^J, i = \overline{1,l}$. В результаті одної й тої ж збурної дії (що відрізняється від стиску з втратами), якій піддалися обидва відповідні зображення, блоки В/ B^J збурилися й стали $B^{(z)}/B^{J(z)}$, нормовані вектори СНЧ яких $\bar{\sigma}^{(z)}/\bar{\sigma}^{J(z)}$. Координати $\bar{\sigma}^{(z)}/\bar{\sigma}^{J(z)}$ позначимо відповідно: $\bar{\sigma}_i{}^{(z)}/\bar{\sigma}_i{}^{J(z)}, i = \overline{1,l}$.

Чутливість нормованого вектора СНЧ оцінюється кутом його повороту в результаті ЗД. Позначимо α' – кут між $\bar{\sigma}$ і $\bar{\sigma}^{(z)}$, а β' – кут між $\bar{\sigma}^J$ і $\bar{\sigma}^{J(z)}$. Тоді:

$$\frac{cos(\alpha')}{cos(\beta')} = \frac{\bar{\sigma}_1\bar{\sigma}_1{}^{(z)} + \bar{\sigma}_2\bar{\sigma}_2{}^{(z)} + \ldots + \bar{\sigma}_l\bar{\sigma}_l{}^{(z)}}{\bar{\sigma}_1{}^J\bar{\sigma}_1{}^{J(z)} + \bar{\sigma}_2{}^J\bar{\sigma}_2{}^{J(z)} + \ldots + \bar{\sigma}_l{}^J\bar{\sigma}_l{}^{J(z)}}.$$

(5.8)

В оригінальному ЦЗ незалежно від його формату (з/без втрат) для більшості блоків його матриці нормований вектор СНЧ близький до вектору e_1 відповідного простору, з чого випливає, що $\bar{\sigma}_1$, $\bar{\sigma}_1^{\,J}$ близькі до одиниці. І хоча збурна дія змінить їх, добутки $\bar{\sigma}_1\bar{\sigma}_1^{(z)}, \bar{\sigma}_1^{\,J}\bar{\sigma}_1^{\,J(z)}$ будуть близькими до 1, порівнянними між собою, а суми інших доданків у випадку різних форматів ЦЗ будуть різними. Дійсно, враховуючи те, що при стиску ЦЗ з втратами зменшується внесок високочастотних (і можливо середньочастотних) складових зображення, основний внесок від яких мають сингулярні трійки, що відповідають найменшим (середнім) за значенням СНЧ блоку, а також добру обумовленість всіх СНЧ, маємо:

$$\bar{\sigma}_2\bar{\sigma}_2^{(z)} + \ldots + \bar{\sigma}_l\bar{\sigma}_l^{(z)} > \bar{\sigma}_2^{\,J}\bar{\sigma}_2^{\,J(z)} + \ldots + \bar{\sigma}_l^{\,J}\bar{\sigma}_l^{\,J(z)},$$

з чого:

$$\bar{\sigma}_1\bar{\sigma}_1^{(z)} + \bar{\sigma}_2\bar{\sigma}_2^{(z)} + \ldots + \bar{\sigma}_l\bar{\sigma}_l^{(z)} > \bar{\sigma}_1^{\,J}\bar{\sigma}_1^{\,J(z)} + \bar{\sigma}_2^{\,J}\bar{\sigma}_2^{\,J(z)} + \ldots + \bar{\sigma}_l^{\,J}\bar{\sigma}_l^{\,J(z)}.$$

(5.9)

З урахуванням (2.19) співвідношення (2.18) буде мати вигляд:

$$\frac{cos(\alpha')}{cos(\beta')} > 1,$$

Звідки

$$\alpha' < \beta',$$

тобто чутливість нормованого вектора СНЧ блоку, що оцінюється кутом його повороту в результаті збурної дії (що відрізняється від стиску з втратами), буде більше для ЦЗ у ФзВ, у порівнянні з чутливістю у відповідному зображення у ФбВ.

Зі зменшенням коефіцієнту якості, використаного при отриманні відповідного ЦЗ у ФзВ з ЦЗ у ФбВ, зменшується $\bar{\sigma}_1^{\,J}\bar{\sigma}_1^{\,J(z)} + \bar{\sigma}_2^{\,J}\bar{\sigma}_2^{\,J(z)} + \ldots + \bar{\sigma}_l^{\,J}\bar{\sigma}_l^{\,J(z)}$, оскільки більша кількість СНЧ стає порівнянною з нулем. Наслідком цього буде зростання

$$\frac{\bar{\sigma}_1\bar{\sigma}_1^{(z)} + \bar{\sigma}_2\bar{\sigma}_2^{(z)} + \ldots + \bar{\sigma}_l\bar{\sigma}_l^{(z)}}{\bar{\sigma}_1^{\,J}\bar{\sigma}_1^{\,J(z)} + \bar{\sigma}_2^{\,J}\bar{\sigma}_2^{\,J(z)} + \ldots + \bar{\sigma}_l^{\,J}\bar{\sigma}_l^{\,J(z)}},$$

що приводить до того, що кут β' буде тим більшим, чим меншим буде QF, тобто чутливість нормованого вектора СНЧ блоку відповідного ЦЗ зростає зі зменшенням коефіцієнта якості, який використовувався при його отриманні, що й потрібно було довести.

Отримані висновки знайшли своє підтвердження на практиці. У результаті обчислювального експерименту, в якому були задіяні 400 ЦЗ в ФбВ з бази img_Nikon_D70s (множина M) і множини відповідних їм зображень, встановлено, що середнє значення кута повороту, отримане в процесі усереднення по всім розглянутим ЦЗ середніх значень по блоках для окремих зображень, для ЦЗ в форматі Jpeg (QF=85), коли як ЗД використовувалося накладання гауссівського шуму з нульовим математичним очікуванням і D=0.0001, на 29% більше відповідного параметра для відповідних ЦЗ в форматі Tif. У випадку, коли як ЗД використовувалося накладання мультиплікативного шуму з D=0.0001, середнє значення розглянутого кута для Jpeg-ЦЗ виявилося більше на 9.7%. Для перевірки

монотонності збільшення кута, що розглядається, зі зменшенням коефіцієнту QF, що використовувався при отриманні відповідних ЦЗ, кожне з зображень з множини M зберігалося в ФзВ з кожним з $QF \in \{65,75,85,95\}$. Результати експерименту наведені на рис.5.3, де очевидна монотонність для кожної з розглянутих збурних дій.

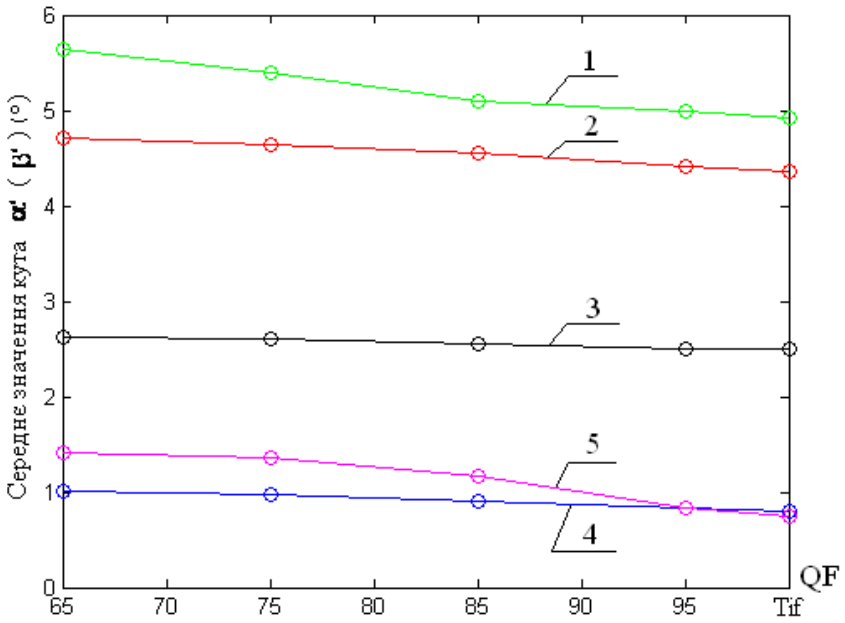


Рис. 5.3. Графіки залежності середнього значення кута α' (для ЦЗ в ФбВ) (β' (для відповідних ЦЗ у ФзВ)), що характеризує чутливість нормованого вектора СНЧ блоку до ЗД, від значення коефіцієнта QF, що використовувався при отриманні відповідних ЦЗ для зображень в ФбВ, коли як ЗД застосовувалося: 1 – накладання пуассонівського шуму; 2 – накладання гауссівського шуму з нульовим маточікуванням і D=0.001; 3 – накладання шуму «сіль-перець» з d=0.05; 4 – накладання мультиплікативного шуму з D=0.001; 5 – стеганоперетворення методом LSB з ПСПК=0.5 біт/піксель

Якщо аналізу піддаються ЦЗ, що не є відповідними, а обрані випадковим чином, у різних форматах (з/без втрат), то чутливість вектора СНЧ для ЦЗ у ФзВ виявляється порівнянною з чутливістю вектора СНЧ для ЦЗ в ФбВ.

2. Дослідження залежності чутливості векторів u_1, v_1 блоку від формату збереження зображення

Важливими для розглянутого підходу формальними параметрами, властивості яких є визначальними для базового співвідношення (3.8), зокрема, чутливість до ЗД, є СНВ u_1, v_1, що відповідають максимальному СНЧ σ_1 блока. Можна показати, що поведінка цих СНВ у процесі збурень ЦЗ аналогічна, тому далі розглядається лівий СНВ u_1. Практично встановлено, що чутливість u_1, яка для нормованого вектора кількісно визначається кутом його повороту в результаті ЗД, не залежить від формату ЦЗ (з/без втрат), більше того, вона не залежить і від значення QF, з яким зберігалося ЦЗ в ФзВ (табл.5.3). У ході експерименту оригінальне ЦЗ (в форматі Tif, Jpeg ($QF \in \{65,75,85\}$)) і відповідне йому збурене за рахунок накладання різних шумів з різними параметрами ЦЗ розбивалися на $4\times4-$блоки. Для кожної пари відповідних блоків у цих парах ЦЗ обчислювалося значення кута між СНВ, що відповідають максимальному СНЧ. Для кожного оригінального ЦЗ визначався середній по

блоках кут при кожній конкретній ЗД. Потім визначалися середні значення кута по всіх зображеннях при кожній конкретній ЗД, які представлені в табл.5.3.

Таблиця 5.3

Середнє по всім ЦЗ з ЕМ значення збурення (в градусах) u_1 в $4\times 4-$блоці зображення при різних ЗД

ЗД \ Формат ЦЗ	Tif	Jpeg QF=85	Jpeg QF=75	Jpeg QF=65
Гауссівський шум (D=0.0001)	1.146	1.147	1.151	1.151
Гауссівський шум (D=0.001)	3.475	3.478	3.480	3.478
Мультиплікативний шум (D=0.0001)	0.220	0.219	0.220	0.219
Мультиплікативний шум (D=0.001)	0.736	0.735	0.736	0.736

Отримані результати чутливості вектора u_1, що не залежать від формату збереження ЦЗ, є практичним підтвердженням наступної теореми.

Теорема. Якщо СНВ відповідає максимальному СНЧ блока, то його чутливість до ЗД не залежить від формату ЦЗ (з/без втрат), від значення коефіцієнта якості QF, з яким зберігалося ЦЗ в ФзВ при отриманні відповідного зображення.

Доказ. Чутливість СНВ u_1 визначається відповідно до формули:

$$\frac{1}{2}sin\,2\theta_1 \le \frac{\|\Delta B\|_2}{svdgap(1,B)},$$

(5.10)

де ΔB – матриця збурення блоку B в результаті ЗД, що зазнало ЦЗ, θ_1 – кут повороту вектора u_1,

$$svdgap(1,B) = \min_{j\neq 1}|\sigma_1 - \sigma_j|$$

(5.11)

– відокремленість СНЧ σ_1 в блоці B.

Формально при одній ЗД чутливість u_1 може відрізнятися тільки тоді, коли для різних форматів збереження ЦЗ (Tif, Jpeg ($QF \ge 65$)) буде відрізнятися відокремленість $svdgap(1,B)$, яка остаточно визначається як

$$svdgap(1,B) = \sigma_1 - \sigma_2$$

(5.12)

в відповідних блоках зображень. Для блоків матриці ЦЗ сингулярний спектр має свої особливості: в блоках оригінальних ЦЗ, незалежно від формату (з/без втрат), максимальне СНЧ значно перевищує всі інші:

$$\sigma_1 >> \sigma_2 \ge \ldots \ge \sigma_l \ge 0,$$

(5.13)

тому можна вважати, що $\sigma_1 - \sigma_2 \approx \sigma_1$. Це приводить до того, що з врахуванням нечутливості СНЧ, відокремленості максимального СНЧ σ_1 в відповідних блоках відповідних зображень, що зберігаються в форматі Tif, Jpeg ($QF \geq 65$), порівнянні між собою. Крім того, враховуючи добру обумовленість СНЧ, оцінку чутливості u_1 можна також проводити відповідно до формули:

$$\frac{1}{2} sin\, 2\theta_1 \leq \frac{\|\Delta B\|_2}{svdgap(1, B + \Delta B)},$$

(5.14)

де в знаменнику дроба в правій частині (5.14) знаходиться відокремленість першого (максимального) СНЧ $B + \Delta B$: $\sigma_1 + \Delta\sigma_1$, де $\Delta\sigma_1$ – збурення σ_1 в результаті ЗД ΔB. Якщо як ЗД для зображення в ФбВ розглянути процес стиску ЦЗ з втратами, то з останньої формули безпосередньо випливає порівнянність чутливостей u_1 в відповідних блоках ЦЗ, збережених в форматі Tif, Jpeg ($QF \geq 65$), при однаковій ЗД. Кут повороту u_1 буде залежити лише від величини ЗД $\|\Delta B\|_2$, що діє на конкретний блок зображення, а не від формату ЦЗ. Таким чином, чутливість СНВ u_1 блоку (як якісно, так і кількісно) не залежить від формату збереження ЦЗ, що й потрібно було довести.

Установлені особливості параметрів блоків ЦЗ приводять до того, що для відповідних ЦЗ у форматах із втратами й без втрат більш чутливою до ЗД (за рахунок нормованого вектора СНЧ) виявиться пара векторів u_1 і $\bar{\sigma}$ в блоках ЦЗ в ФзВ. Підтвердженням цьому є результати наступного обчислювального експерименту. Відповідні ЦЗ в форматах Tif, Jpeg ($QF \in \{65,75,85\}$) піддавалися ЗД, у якості яких використовувалися: накладання гауссівського, мультиплікативного шуму з різними параметрами. Для кожної групи зображень виду: ЦЗ в певному форматі, вони ж після конкретної ЗД, підраховувалася середня по зображеннях кількість блоків (далі позначається T_{60}), для яких кут між u_1 і $\bar{\sigma}$ дорівнював 60 градусам, окремо для оригінальних і окремо для збурених ЦЗ. Результати експерименту, коли як ЗД використовувалося накладання гауссівського шуму з нульовим математичним очікуванням і D=0.0001, представлені в табл.5.4.

Таблиця 5.4

Середнє значення кількості 4×4-блоків, для яких кут між нормованим вектором СНЧ і u_1 дорівнює 60 градусам, в ЦЗ

Формат поданого зображення	Tif	Jpeg QF=85	Jpeg QF=75	Jpeg QF=65
Без ЗД	12776	15816	16161	16675
Після ЗД	8931	9720	9895	10029
Відносне зменшення T_{60} в рез-ті ЗД (%)	30.1	38.5	38.8	39.9

Отримані результати практично підтверджують більш високу чутливість до ЗД пари векторів u_1 і $\bar{\sigma}$ в блоках ЦЗ в ФзВ, у порівнянні з відповідним ЦЗ в ФбВ.

Таким чином для відповідних ЦЗ встановлено:

— співвідношення (3.8) буде виконуватися з більшою точністю для ЦЗ у ФзВ за рахунок меншої відмінності в блоках нормованого вектора СНЧ від вектора e_1, ніж для ЦЗ в ФбВ;

— нормований вектор СНЧ у блоках ЦЗ у ФбВ є менш чутливим до ЗД, ніж у відповідних блоках ЦЗ в ФзВ;

— чутливість лівого (правого) СНВ u_1 (v_1), що відповідають максимальному СНЧ блоків, не залежить від формату збереження ЦЗ;

— менш чутливою до ЗД є пара векторів u_1 і $\overline{\sigma}$ в блоках ЦЗ в ФбВ, ніж в відповідному ЦЗ в ФзВ.

Таким чином, для відповідних ЦЗ ФзВ визначений як такий, для якого (3.8) виконуються з більшою точністю для більшої кількості блоків оригінального ЦЗ та має місце більша чутливість використовуваних формальних параметрів при виявленні ЦЗ, цілісність якого порушена.

Отримані результати для груп відповідних ЦЗ в різних форматах (з/без втрат) доцільно використовувати при розробці методів виявлення ЦЗ, перезбережених із ФзВ у ФбВ, що є актуальним для процесу виявлення ЦЗ, цілісність яких була порушена, зокрема для проведення стеганоаналізу.

Питання

1. Як залежить чутливість векторів $\overline{\sigma}$, u_1, v_1 блоку від формату збереження цифрового зображення? Пояснити.
2. Показати, що нормований вектор сингулярних чисел у блоках цифрового зображення у форматі без втрат є менш чутливим до збурних дій, ніж у відповідних блоках цифрового зображення в форматі з втратами.
3. Показати, що чутливість лівого (правого) сингулярного вектора u_1 (v_1), що відповідає максимальному сингулярному числу блока, не залежить від формату збереження зображення.
4. Показати, що менш чутливою до збурних дій є пара векторів u_1 і $\overline{\sigma}$ в блоках цифрового зображення в форматі без втрат, ніж в відповідному цифровому зображенні в форматі з втратами.

Література

1. Бобок І.І., Кобозєва А.А. Особливості нового підходу до вирішення проблеми виявлення порушень цілісності цифрових зображень в різних форматах збереження. Безпека інформації. 2017. 23(3). С. 197–203 https://core.ac.uk/download/pdf/296366114.pdf
2. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с. https://studizba.com/files/show/pdf/53191-1-dzh-demmel--vychislitel-naya-lineynaya.html
3. И.Бобок, «Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров»,Інформатика та математичні методи в моделюванні, Т.7, No3, С.211-219, 2017.

Лекція 7. УНІВЕРСАЛЬНИЙ МЕТОД ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

План

1.Додатковий аналіз гістограм ГU (ГV)

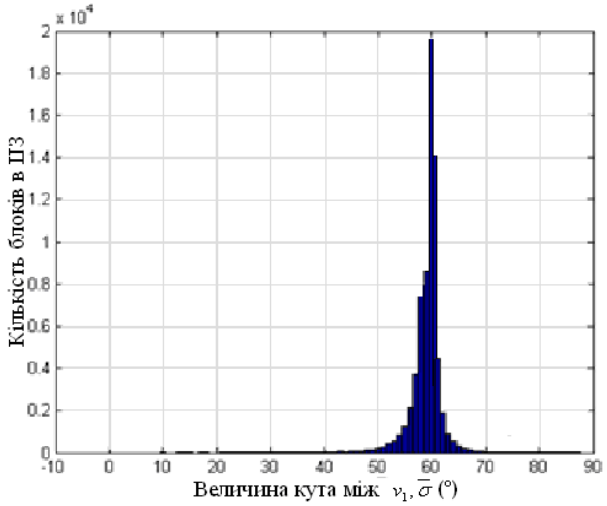
2. Метод виявлення порушення цілісності та його алгоритмічна реалізація

3. Аналіз ефективності методу

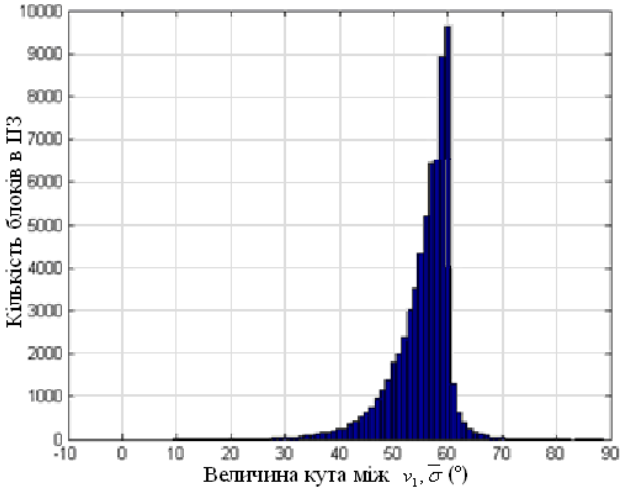
1. Додатковий аналіз гістограм ГU (ГV)

Співвідношення (3.8) (лекція 3-4) характерні для більшості блоків більшості оригінальних ЦЗ. В умовах збурних дій на ЦЗ ці співвідношення можуть порушуватися. Однак, як було показано, з урахуванням лише одного параметра – моди гістограми ГU (ГV) величин кутів між векторами u_1 і $\overline{\sigma}$ (v_1 і $\overline{\sigma}$) $l \times l -$блоків, отриманих у результаті стандартної розбивки матриці зображення, можлива ситуація, коли відокремити оригінальне зображення від неоригінального буде неможливо: аналізовані параметри можуть співпадати (рис. 2.1), а тому для забезпечення можливості відокремлення необхідно підключення додаткових характеристик (гістограм ГU (ГV)) ЦЗ для аналізу при розробці методу виявлення порушень цілісності ЦЗ, заснованого на ЗППЦ.

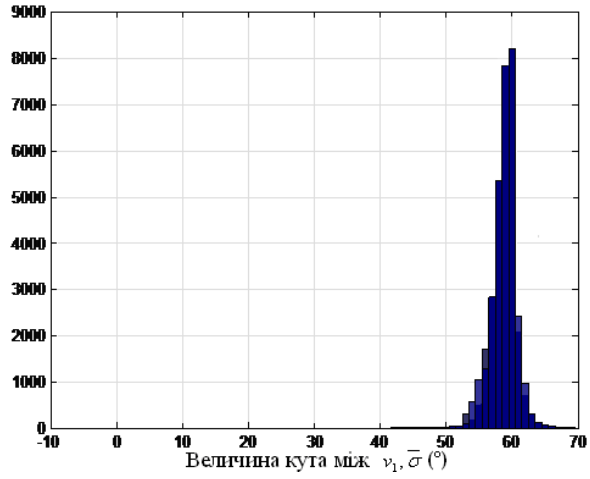
Збурення оригінального ЦЗ приведе до зменшення кількості блоків, у яких рівність в (3.8) буде мати місце, і, як наслідок, може взагалі привести до порушення співвідношення (3.8) для більшості блоків ЦЗ, коли мода гістограми ГU (ГV) не буде дорівнювати $\angle(n^O, e_1)$. Але, якщо (3.8) і буде мати місце для збуреного ЦЗ, то результат збурення формально відобразиться в зменшенні значення глобального максимуму ГU (ГV) для збуреного ЦЗ, в порівнянні з оригінальним і, як наслідок, в «розширенні» самої гістограми в околі моди ГU (ГV) (рис.7.1, 7.2, 7.3 (б, в); тут в якості збурних дій для ЦЗ навмисно обиралися різні: накладання шумів (гауссівського, мультиплікативного з різними параметрами, пуассонівського), стеганоперетворення за допомогою LSB-методу). Дійсно, при збуренні ЦЗ збурення отримують і u_1, і $\overline{\sigma}$ (v_1 і $\overline{\sigma}$), що приведе до того, що деякі блоки, для яких до збурення $\angle(u_1, \overline{\sigma}) = \angle(n^O, e_1)$ ($\angle(v_1, \overline{\sigma}) = \angle(n^O, e_1)$) після збурення вже такими не будуть і не дадуть свій внесок у стовпчик гістограми, який відповідає $\angle(n^O, e_1)$.



а



б



в

Рис. 7.1. Гістограми ГV (для блоків 4×4) конкретного ЦЗ (формат Tif): а – оригінальне ЦЗ; б – ЦЗ після накладання гауссівського шуму з нульовим математичним очікуванням і D = 0.001); в – ЦЗ-стеганоповідомлення, сформоване стеганографічним методом LSB з пропускною спроможністю прихованого каналу зв'язку 0.75 біт/піксель

Враховуючи нечутливість до збурних дій векторів u_1, v_1, $\bar{\sigma}$, їх збурення не можуть бути значними, тобто кут $\angle(u_1,\bar{\sigma})$ ($\angle(v_1,\bar{\sigma})$) хоч і зміниться і не буде дорівнювати $\angle(n^O,e_1)$, але не може відрізнятися від $\angle(n^O,e_1)$ значно, а це означає, що такі блоки, забравши свій внесок зі стовпчика гістограми, який відповідає $\angle(n^O,e_1)$, перенесуть цей внесок у прилеглі стовпчики гістограми (в околі моди), збільшуючи їх, що і приведе до її «розширення», яке кількісно може бути оцінено за допомогою відношення кількості блоків зображення, для яких $\angle(u_1,\bar{\sigma})$ ($\angle(v_1,\bar{\sigma})$) знаходиться в малому околі $\angle(n^O,e_1)$, до значення гістограми ГU (ГV) в моді: чим більше значення вказаного відношення, тим більше ймовірність того, що зображення, що піддається експертизі, є таким, цілісність якого порушена.

Конкретика збурної дії (що відрізняється від стиску з втратами) не впливає якісно на характер зміни гістограми збуреного ЦЗ в порівнянні з оригінальним, який не залежить також від розміру блоків, на які розбивається матриця аналізованого ЦЗ, ілюстрацією чому є рис. 7.1, 7.2, 7.3, де для кожного виду збурення та для кожного розміру блоку, що використовувався, в результаті збурної дії значення гістограми в моді зменшується, гістограма «розширюється», тобто більша кількість блоків зображення буде мати кути між векторами u_1 і $\bar{\sigma}$ (v_1 і $\bar{\sigma}$), значення яких незначно відрізняється від $\angle(n^O,e_1)$ в відповідному просторі, в порівнянні з оригінальним зображенням. Крім цього, для збуреного ЦЗ мода ГU (ГV) може зсуватися відносно її положення в оригінальному ЦЗ та відносно значення $\angle(n^O,e_1)$.

Характер зміни поведінки ГU, ГV в результаті збурної дії, яка відрізняється від стиску з втратами, не залежить від формату (з/без втрат) ЦЗ, що піддавалося цій збурній дії.

Для практичного підтвердження отриманого висновку розглядалися й порівнювалися безпосередньо гістограми ГU (ГV) оригінальних (500 ЦЗ в форматах Jpeg і Tif) й збурених ЦЗ (500 ЦЗ, що отримувалися за допомогою різноманітних збурних дій над оригінальними зображеннями: накладання гауссівського, мультиплікативного шумів з різними параметрами, пуассонівського шуму, стеганоперетворення ЦЗ за допомогою LSB-методу з пропускною спроможністю прихованого каналу зв'язку 0.75, 1 біт/піксель, стеганоперетворення за допомогою методу Коха і Жао).

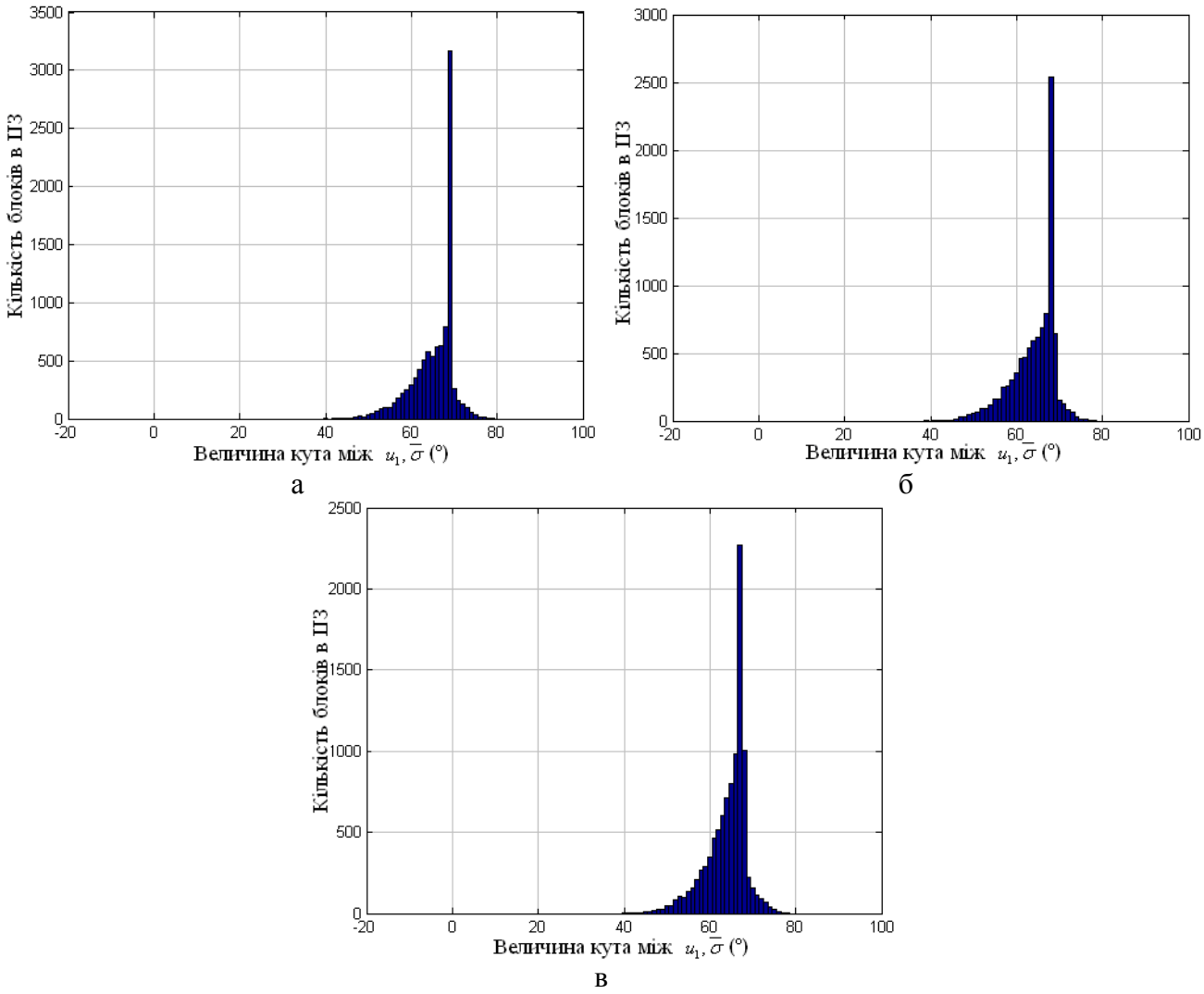


Рис. 7.2. Гістограми ГU (для блоків 8×8) конкретного ЦЗ (формат Jpeg): а – оригінальне ЦЗ; б – зашумлене ЦЗ (гауссівський шум з нульовим математичним очікуванням і $D = 0.001$); в – зашумлене ЦЗ (мультиплікативний шум з $D = 0.005$)

Значення глобального максимуму ГU (ГV) для оригінальних ЦЗ часто приблизно в 1.5-2 рази більше, ніж для відповідних збурених; гістограма для збуреного ЦЗ «ширша» гістограми для оригінального. Таким чином, у якості додаткового кількісного параметра для відокремлення оригінального ЦЗ від неоригінального може виступати відношення кількості блоків ЦЗ, для яких кути між векторами u_1 і $\overline{\sigma}$ (v_1 і $\overline{\sigma}$) знаходяться в деякому околі $\angle(n^O, e_1)$ незначного радіуса, до значення ГU (ГV) в моді гістограми (що і буде кількісно характеризувати «розширення» гістограми).

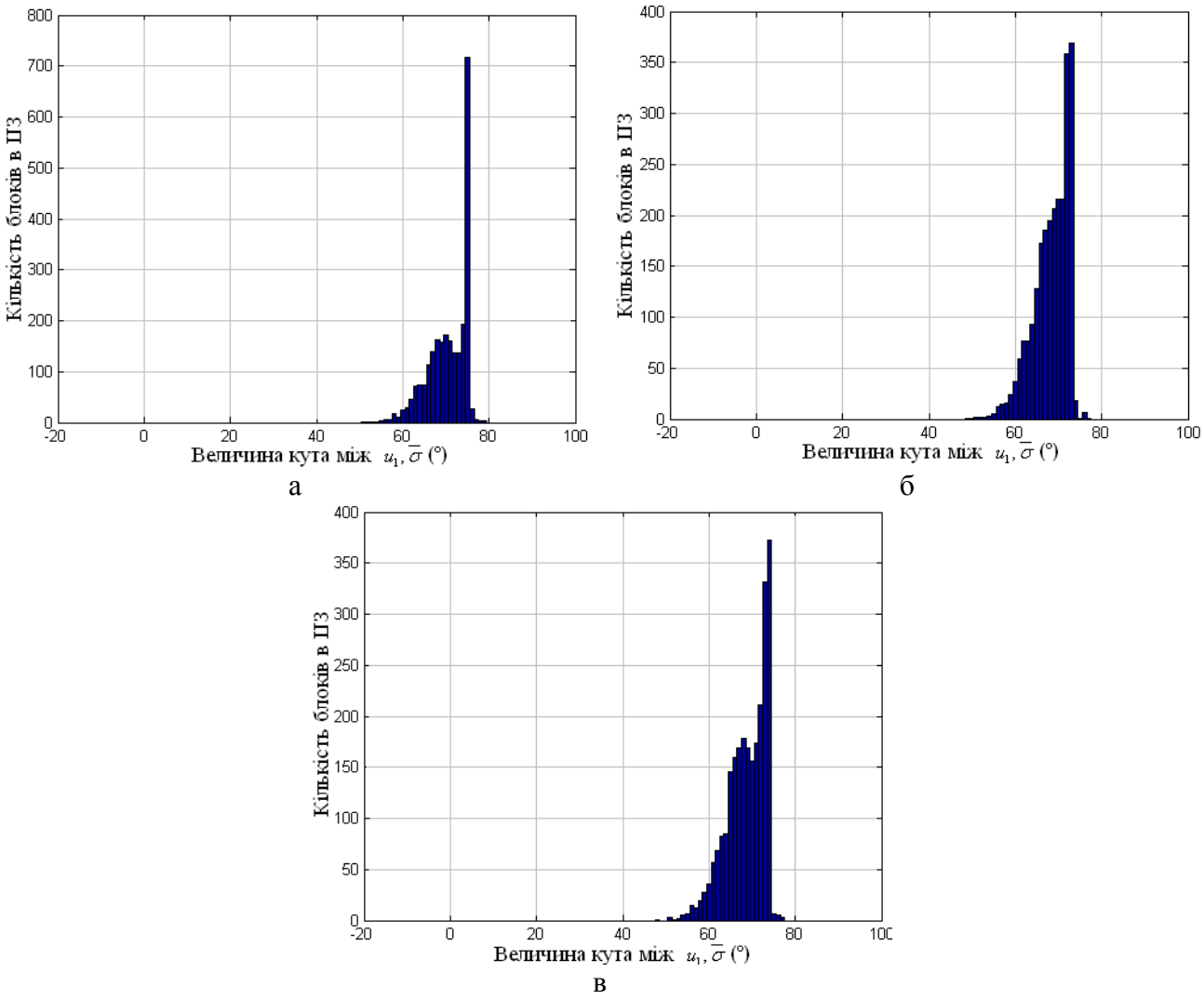


Рис. 7.3. Гістограми ГU (для блоків 16×16) конкретного ЦЗ (формат Jpeg): а – оригінальне ЦЗ; б – зашумлене ЦЗ (мультиплікативний шум з $D = 0.01$); в – зашумлене ЦЗ (пуассонівський шум)

Отримані якісні характеристики дозволяють відрізнити оригінальне ЦЗ від збуреного навіть при співпадінні мод ГU, ГV (можливість чого відзначалася в підрозділі 2.1 як недолік ЗППЦ).

2. Метод виявлення порушення цілісності та його алгоритмічна реалізація

Усе вищесказане може бути використане для розробки методів виявлення порушення цілісності ЦЗ. У якості основних кроків одного з таких методів, названого KBG, виступають наступні.

Крок 1. Аналізоване ЦЗ розбивається стандартним чином на $l \times l$-блоки.

Крок 2. Для кожного з отриманих $l \times l$-блоків B знайти $\angle(u_1, \bar{\sigma})$, $\angle(v_1, \bar{\sigma})$.

Крок 3. Для аналізованого ЦЗ побудувати гістограми ГU, ГV з кроком h.

Крок 4. Для ГU, ГV визначити моди A_U, A_V, а також значення M_U, M_V гістограм в модах відповідно.

Крок 5. Для аналізованого ЦЗ з використанням ГU, ГV обчислити відповідно кількості S_U, S_V блоків, для яких $\angle(u_1, \bar{\sigma}) \in [\angle(n^O, e_1) - T, \angle(n^O, e_1) + T]$,

$\angle(v_1,\bar{\sigma})\in[\angle(n^O,e_1)-T,\angle(n^O,e_1)+T]$, де T – параметр, що визначається експериментально.

Крок 6 (перевірка).

Якщо

$$\left(A_U\notin\left\{\angle(n^O,e_1)-1,\angle(n^O,e_1),\angle(n^O,e_1)+1\right\}\right)\vee$$
$$\vee\left(A_V\notin\left\{\angle(n^O,e_1)-1,\angle(n^O,e_1),\angle(n^O,e_1)+1\right\}\right),$$

то

для аналізованого ЦЗ цілісність порушена.

Якщо

$$\left(A_U,A_V\in\left\{\angle(n^O,e_1)-1,\angle(n^O,e_1),\angle(n^O,e_1)+1\right\}\right)\&\left((S_U/M_U>P_U)\vee(S_V/M_V>P_V)\right),$$

де P_U, P_V – порогові значення, що визначаються експериментально,

то

для аналізованого ЦЗ цілісність порушена.

Якщо

$$\left(A_U,A_V\in\left\{\angle(n^O,e_1)-1,\angle(n^O,e_1),\angle(n^O,e_1)+1\right\}\right)\&(S_U/M_U\le P_U)\&(S_V/M_V\le P_V),$$

то

для аналізованого ЦЗ цілісність не порушена.

Дальнейшие результаты приводятся для реализации метода при следующих значения параметров: $T=15^o$, $P_U=P_V=3.2$. Для удобства обозначим: $k_U=S_U/M_U$, $k_V=S_V/M_V$.

3. Аналіз ефективності методу

Проілюструємо роботу алгоритмічної реалізації розробленого методу на двох ЦЗ, що зберігаються в різних форматах: Lenna (без втрат) (рис. 7.4(а)), Owlet (з втратами) (рис. 7.4(б)), взятих із традиційно використовуваних при тестуванні різних алгоритмів баз ЦЗ.

а

б

Рис. 7.4. Тестові ЦЗ: а – Lenna; б – Owlet

Як видно з результатів, наведених у табл. 7.1, 7.2, застосування запропонованих кількісних параметрів дозволяє відокремити оригінальне ЦЗ від зображення, цілісність якого порушена за рахунок збурних дій, відмінних від стеганоперетворення, а також за рахунок вбудови додаткової інформації різними стеганографічними алгоритмами. Навіть у випадку,

коли $A_U = A_V = 60^\circ$ (наприклад, випадок накладення на ЦЗ шуму «salt & pepper»), безпосереднє якісне порівняння гістограм ГU, ГV оригінального й збуреного ЦЗ з урахуванням вищесказаного дає можливість для їхньої класифікації (рис. 7.5), яка підтверджується додатковими кількісними параметрами k_U і k_V, для яких: $k_U \geq P_U$, $k_V \geq P_V$.

Як ілюструють табл. 7.1,7.2, правильність результату роботи алгоритмічної реалізації KBG при відокремленні оригінального ЦЗ від зображення, цілісність якого порушена, не залежить від формату (з/без втрат) вхідного зображення, специфіки використаних стеганографічних алгоритмів, особливостей і параметрів шумів, що накладаються на зображення: усі варіанти зображень, для яких цілісність була порушена, були виявлені методом KBG, правильно класифікувалися також оригінальні зображення.

Таблиця 7.1

Результати аналізу за допомогою KBG тестових ЦЗ в умовах порушення цілісності за рахунок збурних дій, відмінних від стеганоперетворення (результати представлені у вигляді: $A_U / k_U \left(A_V / k_V \right)$)

ЦЗ	ГU								ГV							
	Оригінальне ЦЗ	Збурні дії							Оригінальне ЦЗ	Збурні дії						
		Gaussian		Speckle		Salt & Pepper		poisson		Gaussian		Speckle		Salt & Pepper		poisson
		D=10-3	D=10-4	D=10-2	D=10-3	d=0.02	d=0.05			D=10-3	D=10-4	D=10-2	D=10-3	d=0.02	d=0.05	
Lenna	60 / 3.13	58 / 5.91	59 / 4.20	57 / 6.16	59 / 5.05	60 / 4.67	59 / 6.30	57 / 6.39	60 / 3.07	58 / 5.65	59 / 4.32	57 / 5.98	59 / 5.08	60 / 4.58	60 / 6.17	57 / 6.45
Owlet	60 / 3.01	55 / 10.6	59 / 4.46	57 / 5.56	59 / 3.24	60 / 3.71	60 / 5.02	57 / 7.97	60 / 3.04	56 / 9.94	59 / 4.34	57 / 5.67	60 / 3.29	60 / 3.79	60 / 5.11	57 / 7.89

Таблиця 7.2

Результати аналізу за допомогою KBG тестових ЦЗ в умовах порушення цілісності за рахунок стеганоперетворення різними стеганоалгоритмами (результати представлені у вигляді: $A_U / k_U \left(A_V / k_V \right)$)

ЦЗ	ГU										ГV									
	Стеганоалгоритми і їх параметри										Стеганоалгоритми і їх параметри									
	LSB-matching			LSB-replacement			Куттера-Джордана-Боссена		Коха и Жао		LSB-matching			LSB-replacement			Куттера-Джордана-Боссена		Коха и Жао	
	ПСПК (біт/піксель)			ПСПК (біт/піксель)							ПСПК (біт/піксель)			ПСПК (біт/піксель)						
	0.5	0.75	1	0.5	0.75	1	v=0.01	v=0.05	p=40	p=35	0.5	0.75	1	0.5	0.75	1	v=0.01	v=0.05	p=40	p=35
Lenna	60 / 3.77	60 / 3.79	60 / 3.84	60 / 3.68	59 / 3.69	59 / 3.74	58 / 4.91	57 / 5.90	58 / 5.10	58 / 5.01	60 / 3.81	59 / 3.84	59 / 3.90	60 / 3.57	59 / 3.56	59 / 3.61	58 / 4.94	57 / 5.41	58 / 4.98	58 / 4.88

Owlet	60 3.94	60 3.95	59 3.98	59 3.91	59 3.92	59 3.93	57 4.87	57 5.38	58 4.77	58 4.65	59 3.90	60 3.92	59 3.94	60 3.89	59 3.91	59 3.94	58 4.74	57 5.47	58 4.76	58 4.31

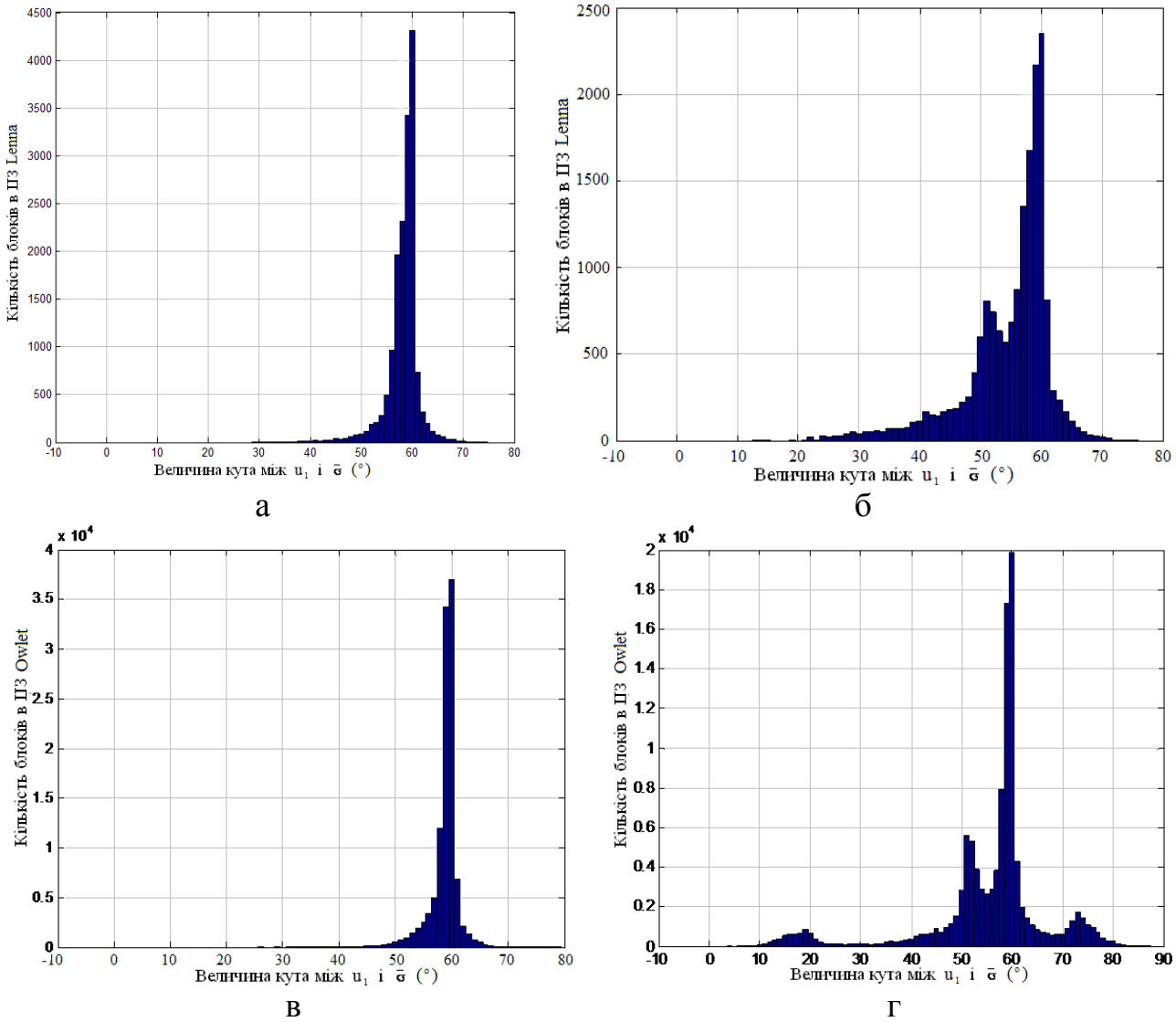


Рис. 7.5. Гістограми ГУ: а – для оригінального ЦЗ Lenna; б – для ЦЗ, отриманого накладанням шуму «salt & pepper» (d=0.02) на ЦЗ Lenna; в – для оригінального ЦЗ Owlet; г – для ЦЗ, отриманого накладанням шуму «salt & pepper» (d=0.02) на ЦЗ Owlet

Таким образом, рассмотренный метод, благодаря использованию универсального математического аппарата при его создании, является эффективным при выявлении не только результатов стеганопреобразования, но и результатов других возмущающих воздействий, изменяющих ЦИ.

Питання

1. Метод виявлення порушення цілісності цифрового зображення.
2. Алгоритмічна реалізація методу виявлення порушення цілісності цифрового зображення.
3. В чому полягає особливість методу виявлення порушення цілісності цифрового зображення, яка робить його універсальним?

4. Оцінка ефективності алгоритмічної реалізації методу.

Література

1. Кобозева А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. Праці Одеського політехнічного університету. 2014. 2. С. 136–146.
2. Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. Transport and Telecommunication Journal. 2016. 17(2). P. 128–137. http://dspace.opu.ua/jspui/bitstream/123456789/4003/1/Bobok_ttj-2016-0012.pdf

ЗМІСТОВИЙ МОДУЛЬ 2. ЗАСТОСУВАННЯ ЗАГАЛЬНОГО ПІДХОДУ ДО АНАЛІЗУ ІНФОРМАЦІЙНИХ СИСТЕМ В СТЕГАНОГРАФІЇ

Лекція 8. ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СПРИЙНЯТТЯ СТЕГАНОПОВІДОМЛЕННЯ

План

1. Стеганоперетворення як збурення набору параметрів, що визначають основне повідомлення
2. Вплив норми матриці збурення на процес забезпечення надійності сприйняття стеганоповідомлення

1. Стеганоперетворення як збурення набору параметрів, що визначають основне повідомлення.

У даний момент в усьому світі назріло питання розробки нових і вдосконалювання існуючих методів захисту інформації, представленої в цифровому виді, серед яких важливе місце займають методи цифровий стеганографії. В основі багатьох підходів до розв'язку задач стеганографії лежить загальна із криптографією методична база, яку заклав ще в середині минулого століття К. Шеннон. Однак і дотепер теоретичні основи стеганографії залишаються недостатньо проробленими.

Завдання вбудовування й виділення повідомлень із іншої інформації виконує стеганосистема, яка, як правило, складається з основних елементів, представлених на рис.8.1.

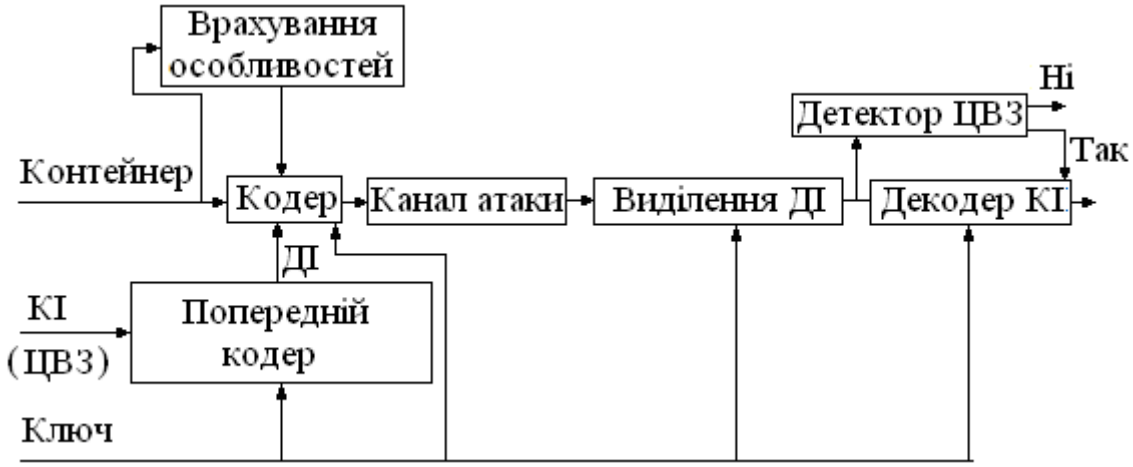


Рис.8.1 – Схема типової стеганосистеми

Процес вбудови додаткової інформації (ДІ) в основне повідомлення (ОП), або контейнер, називається стеганоперетворенням (СПр), а результат СПр — стеганоповідомленням (СП).

Розглянемо докладно процес стеганоперетворення дискретного двовимірного сигналу (ЦЗ або кадра цифрового відео).

У якості ОП, не обмежуючи спільності міркувань, для простоти викладу розглядається зображення з матрицею F.

Перетворення ОП за рахунок вбудови в нього ДІ, незалежно від способу й області цієї вбудови, можна представити як збурення $\Delta F = f(F)$ матриці F, розглядаючи $\overline{F}$ як матрицю СП: $\overline{F} = F + \Delta F$.

Из формулы (1.2) (лекція 1-2), яка розглядається як матричне представлення для СПр, випливає, що довільне СПр можна представити у вигляді аддитивної вбудови деякої інформації в просторовій області.

Будь-які перетворення, які проводяться над СП, будемо розглядати як додаткові збурення матриці ОП F. Відповідно до попередніх лекцій:

- СПр вхідного ОП, а також будь-які перетворення СП при його пересиланні або зберіганні, включаючи активні атакуючі дії, представляються у вигляді елементарних матричних операцій.
- Довільне СПр представляється у вигляді збурення СНЧ і (або) СНВ матриці ОП, що визначаються нормальним сингулярним розкладанням матриці (рис.8.2);
- СПр представляється у вигляді збурення спектра й (або) ВВ матриці ОП, що визначаються нормальним спектральним розкладанням, у випадку симетричної матриці контейнера.

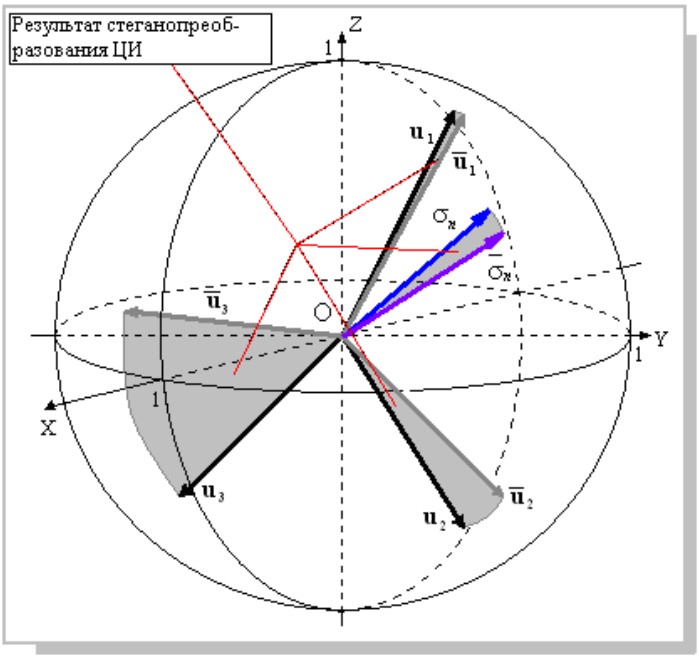


Рис.8.2. Геометричне представлення стеганоперетворення ЦЗ

Основною задачею будь-якого стеганоалгоритма є забезпечення збереження в секреті наявності таємного каналу передачі інформації, інакше кажучи, згенероване стеганографічним алгоритмом СП повинно зберігати надійність сприйняття: спотворення ОП за рахунок вбудови ДІ не повинно бути помітним. Таким чином, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги.

2. Вплив норми матриці збурення на процес забезпечення надійності сприйняття стеганоповідомлення

Базисним перетворенням, що використовуються в багатьох сучасних алгоритмах стиску графічної інформації, а також стеганографічних алгоритмах, є дискретне косинусне перетворення (ДКП), яке можемо записати в матричній формі

$$S = C_N X C_N^T, \tag{8.1}$$

де X — фрагмент поданого зображення розміру $N \times N$,

C — N×N-матриця ДКП, елементи $C(i, j),\ i, j = 0,1,...,N-1$ якої обчислюються за формулою:

$$C(i,j)=\begin{cases}\dfrac{1}{\sqrt{N}}, & \text{при } i=0;\\ \sqrt{\dfrac{2}{N}}\cos(2j+1)\cdot i\cdot\pi, & \text{при } i>0.\end{cases}$$

У результуючій матриці S (8.1) ДКП має місце наступний розподіл частотних складових, схематично показаний на рис. 8.3.

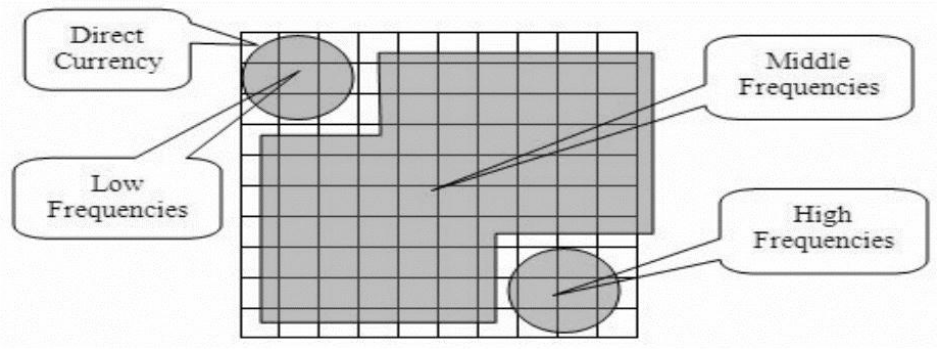


Рис. 8.3. Розподіл частотних складових у трансформантах ДКП

Загальновідомо, що модифікація високочастотних складових (розташованих у нижньому правому куті матриці трансформант ДКП) веде до найменших візуальних спотворень вхідного зображення, тоді як модифікація середніх частот відповідає більшим спотворенням. Найбільші спотворення вхідного зображення відбуваються при модифікації низькочастотних складових (лівий верхній кут) матриці трансформант ДКП.

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

$$SNR=\frac{\|F\|_F^2}{\|\Delta F\|_F^2};\quad PSNR=\frac{n^2\max\limits_{i,j} f_{ij}^2}{\|\Delta F\|_F^2};\quad IF=1-\frac{\|\Delta F\|_F^2}{\|F\|_F^2},\quad SS=1-\frac{\|\Delta F\|_2}{\|F\|_2} \qquad (8.2)$$

де $\|\bullet\|_F$ — матрична норма Фробеніуса, хоча слабкі місця таких показників давно відомі (наприклад, відсутність кореляції цих показників із зором людини). Це пояснюється тим, що всі існуючі моделі зорового сприйняття є лише частковим відбиттям 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. Особливо яскраво така недосконаліть проявляється у випадках, коли зміни цифрового контенту відбуваються в його локальних (малих по розміру) областях. Тут формальна кількісна оцінка спотворення може бути задовільною при явній наявності артефактів (рис.8.4(б)), у той час як значення різницевих показників у випадку відсутності явних візуальних спотворень можуть бути низькими (рис.8.4(в)).

а б в

Рис.8.4. Ілюстрація недосконалості різницевих показників для оцінки візуальних спотворень ЦИ: а - вхідне ЦЗ, б - спотворене ЦЗ (PSNR = 52 dB), в - спотворене за допомогою гауссовського шума ЦЗ (PSNR = 28 dB)

В існуючих стеганометодах часто зустрічаються обмеження на область їх застосовності саме через те, що для якихось ЦЗ-контейнерів надійність сприйняття формованого СП може порушуватися. Це найчастіше відбувається в силу того, що при розробці стеганоалгоритма не враховуються достатні формальні умови такого забезпечення (або такі формальні умови у використовуваній області контейнера не знайдені), а оцінка надійності сприйняття робиться вже апостеріорно, по факту. Така ситуація не дає повною мірою можливості використання випадкового контейнера, є недоліком цих методів.

Оскільки СПр ОП, а також збурні дії, яким зазнає СП, повинні забезпечувати надійність його сприйняття, то $\|\Delta F\|$ не може бути нескінченно великою, де ΔF — матриця збурення ОП або СП, оскільки у цьому випадку достовірною подією виявиться порушення висунутої вимоги. Крім того, при $\|\Delta F\| \to 0$ імовірність забезпечення надійності сприйняття буде прямувати до одиниці для кожного ОП. Значення різницевих показників (8.2) для зображення з матрицею F визначаються величиною $\|\Delta F\|_F$: чим менше $\|\Delta F\|_F$, тим краще кількісний показник візуального спотворення F, що отримується при використанні кожного з них. Враховуючи це, висувається наступна гіпотеза, яка підтверджується обчислювальним експериментом: чим менше $\|\Delta F\|_F$, тим більше ймовірність забезпечення надійності сприйняття для зображення з матрицею $F + \Delta F$ при заданому зображенні F, до того ж замість $\|\Delta F\|_F$ можна використовувати $\|\Delta F\|_2$ - спектральна матрична норма.

Експеримент проводився з використанням 1000 різноманітних по контрастності й по жанру зображень однакового розміру (300×300 пікселів). Збурення зображення проводилося за допомогою накладення шуму (аддитивного гауссовського, мультиплікативного) з різними характеристиками, фільтрації з різними фільтрами. Результати обчислювального експерименту наведені на рис.8.5 ($V = \frac{H}{H_O} \cdot 100\%$, де H — кількість збурених зображень, для яких зберігалася надійність сприйняття, яка встановлювалася за допомогою суб'єктивного ранжирування, H_O — загальне число зображень). Таким чином, для забезпечення високої ймовірності збереження надійності сприйняття СП при заданому контейнері стеганоалгоритм повинен забезпечувати малу норму (зокрема, Фробеніуса, СМН) матриці збурення при СПр.

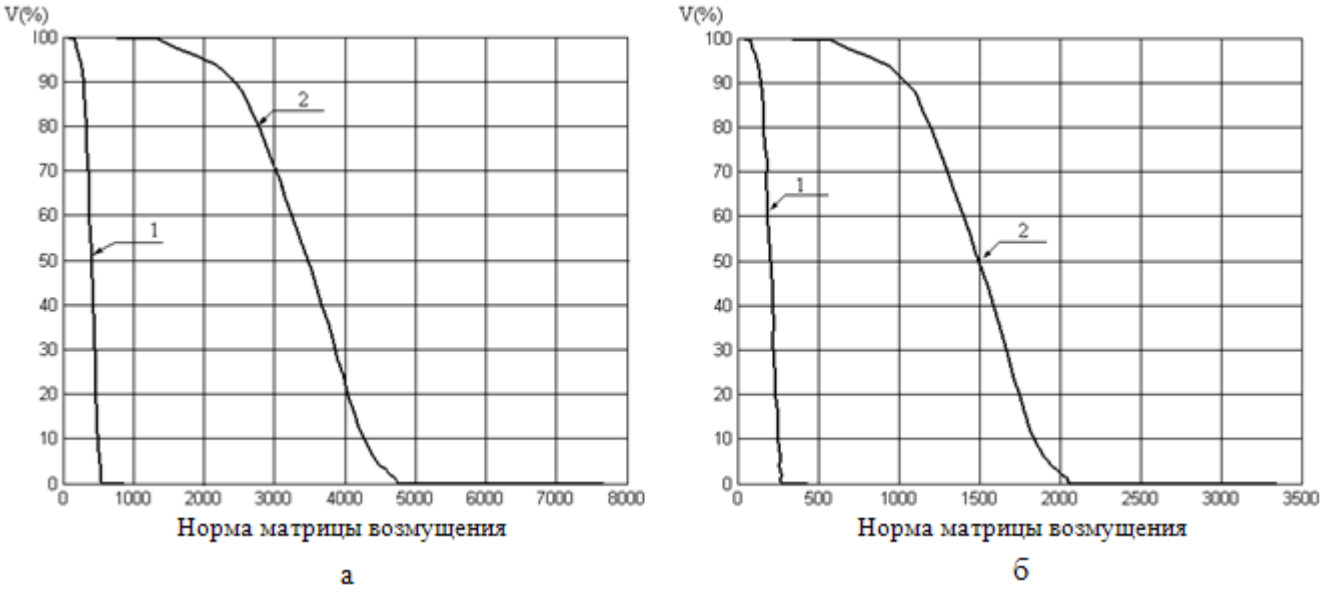


Рис.8.5. Залежність V (%) від норми матриці збурної дії, що є аддитивним гауссовським шумом (а): 1—СМН; 2—норма Фробеніуса; мультиплікативним шумом (б): 1—СМН; 2—норма Фробеніуса

Твердження. При малих збурних діях показник SS є більш чутливим до цих збурень, ніж IF.

Ілюстрацією твердження є рис.8.6, де показник SS вказує на порушення цілісності поданого зображення.

а

IF =

1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
0.9999	1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000
0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1.0000	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
0.9999	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9999
1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

в

б

SS =

0.9959	0.9959	0.9965	0.9961	0.9960	0.9967	0.9966	0.9967	0.9960	0.9966	0.9969	0.9966	0.9963
0.9964	0.9964	0.9959	0.9958	0.9951	0.9961	0.9962	0.9968	0.9954	0.9958	0.9969	0.9969	0.9965
0.9964	0.9964	0.9958	0.9965	0.9964	0.9961	0.9962	0.9966	0.9964	0.9953	0.9969	0.9960	0.9959
0.9962	0.9962	0.9962	0.9954	0.9965	0.9962	0.9961	0.9960	0.9969	0.9973	0.9965	0.9962	0.9971
0.9957	0.9955	0.9968	0.9965	0.9969	0.9959	0.9963	0.9965	0.9966	0.9973	0.9966	0.9967	0.9966
0.9959	0.9963	0.9963	0.9961	0.9961	0.9964	0.9964	0.9964	0.9962	0.9969	0.9966	0.9963	0.9962
0.9959	0.9966	0.9960	0.9963	0.9965	0.9963	0.9959	0.9964	0.9962	0.9956	0.9969	0.9965	0.9962
0.9963	0.9967	0.9968	0.9965	0.9960	0.9965	0.9954	0.9962	0.9961	0.9954	0.9966	0.9966	0.9968
0.9960	0.9966	0.9966	0.9962	0.9968	0.9961	0.9964	0.9963	0.9964	0.9968	0.9971	0.9966	0.9966
0.9964	0.9963	0.9964	0.9964	0.9956	0.9966	0.9954	0.9968	0.9962	0.9966	0.9973	0.9968	0.9967
0.9967	0.9958	0.9964	0.9966	0.9962	0.9963	0.9961	0.9970	0.9972	0.9967	0.9969	0.9967	0.9957
0.9957	0.9960	0.9966	0.9966	0.9965	0.9967	0.9968	0.9971	0.9974	0.9969	0.9976	0.9961	0.9953
0.9961	0.9966	0.9954	0.9964	0.9963	0.9961	0.9970	0.9966	0.9970	0.9956	0.9967	0.9964	0.9957

г

Рис.8.6. Порівняння використання показників IF і SS: а - подане ЦЗ; б - зашумлене ЦЗ; в - матриця блокових значень показника IF; г - матриця блокових значень показника SS

Питання

1. Яким чином стеганоперетворення можна представити у вигляді елементарних матричних операцій? Пояснити.
2. Яке стеганоповідомленя називається чутливим до збурних дій?
3. Вплив норми матриці збурення на процес забезпечення надійності сприйняття стеганоповідомлення.
4. Кількісні різницеві показники надійності сприйняття стеганоповідомлення, їх недоліки.

Література

Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.

Лекція 9. ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СПРИЙНЯТТЯ СТЕГАНОПОВІДОМЛЕННЯ (продовження)

План

1. Умови забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера
2. Відповідність між параметрами двовимірного сигналу в різних областях перетворення

1. Умови забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера

Розглядаючи матрицю ОП як симетричну (див. лекцію 1-2), позначимо її A, щоб відрізняти від довільної матриці F.

Теорема 1. Нехай вбудова ДІ викликає збурення $\delta_{k_1},\dots,\delta_{k_p}$ ВЗ $\lambda_{k_1},\dots\lambda_{k_p}$ матриці A ОП. Тоді величина норми матриці збурення ΔA не залежить від того, які саме ВЗ були збурені, а залежить лише від абсолютних величин цих збурень.

Доказ. Позначимо $\overline{A}$ матрицю СП, що отримане на основі A. Якщо $A=U\Lambda U^T$ - спектральне розкладання матриці контейнера, яке може бути представленим у формі зовнішніх добутків (1.8) $A=\sum_{i=1}^{n}\lambda_i u_i u_i^T$ (див. лекція 1-2), то спектральне розкладання матриці СП $\overline{A}$ буде мати вигляд:

$$\overline{A}=U\,diag(\lambda_1,\dots,\lambda_{k_1-1},\lambda_{k_1}+\delta_{k_1},\lambda_{k_1+1},\dots,\lambda_{k_p-1},\lambda_{k_p}+\delta_{k_p},\lambda_{k_p+1},\dots\lambda_n)U^T.$$

Тоді, враховуючи (1.8),

$$\Delta A=\overline{A}-A=\sum_{j=1}^{p}\delta_{k_j}u_{k_j}u_{k_j}^T,\quad \|\Delta A\|_2=\max_{1\le j\le p}\left|\delta_{k_j}\right|.$$

Зв'язок між $\|\Delta A\|$ і $\delta_{k_1},\dots,\delta_{k_p}$ залежить від вибору матричної норми. Наприклад, якщо розглянути норму Фробеніуса, то

$$\|\Delta A\|_F=\left\|\sum_{j=1}^{p}\delta_{k_j}u_{k_j}u_{k_j}^T\right\|_F\le\sum_{j=1}^{p}\left|\delta_{k_j}\right|\left\|u_{k_j}\right\|_2\left\|u_{k_j}^T\right\|_2=\sum_{j=1}^{p}\left|\delta_{k_j}\right|\le p\max_{1\le j\le p}\left|\delta_{k_j}\right|,$$

висновок теореми істинний.

Теорема 2. Нехай СПр викликало збурення ВВ матриці A ОП. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених ВВ малим по модулю ВЗ A.

Без доказу.

Нехай ΔA — збурення матриці A тільки за рахунок збурення ВВ, $u_i,\overline{u_i}$ — нормовані даний і збурений ВВ, що відповідають λ_i, а θ_i — кут між ними.

Теорема 3. Нехай СПр збурило ВВ матриці A ОП. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених ВВ власним значенням матриці ОП із малою абсолютною відокремленістю.

Доказ. Оскільки нерівність (1.10) (див. лекц.1-2) має місце для кожного ВЗ матриці A, то

$$\max_{1\le i\le n}\left(\frac{1}{2}\sin\theta_i\ gap_{abs}(i,A)\right)\le\|\Delta A\|_2, \qquad (9.1)$$

звідки випливає висновок теореми. З формули (9.1) випливає, що якщо при збуренні вхідної матриці A її ВЗ не міняються або міняються незначно, то навіть великі збурення ВВ, що відповідають погано абсолютно відокремленим СЗ ($gap_{abs}(i,A)$ мала), приведуть до малого значення $\|\Delta A\|_2$.

З метою забезпечення великої ймовірності надійності сприйняття СП вбудову ДІ в контейнер доцільно робити таким чином, щоб збурені стеганоперетворенням ВВ відповідали малим по модулю ВЗ або ВЗ, що мають малі абсолютні відокремленості, збурення ВЗ були малі. Чим менше збурення ВЗ, абсолютні відокремленості й модулі ВЗ, що відповідають збуреним ВВ, тим більше ймовірність дотримання надійності сприйняття СП.

Аналогічна умова може бути отримана для контейнера з довільною матрицею з використанням її СНЧ і СНВ (див. «Методичні вказівки до лабораторних робіт»).

2. Відповідність між параметрами двовимірного сигналу в різних областях перетворення

Визначення. Назвемо

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

апроксимацією ранга k зображення F,

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

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.9.1). Результати візуально аналогічні результатам низькочастотної (рис.9.1(б,в)) і високочастотної фільтрації (рис.9.1(д,е)). Варіанти а і г (рис.9.1) наочно не відрізняються один від іншого.

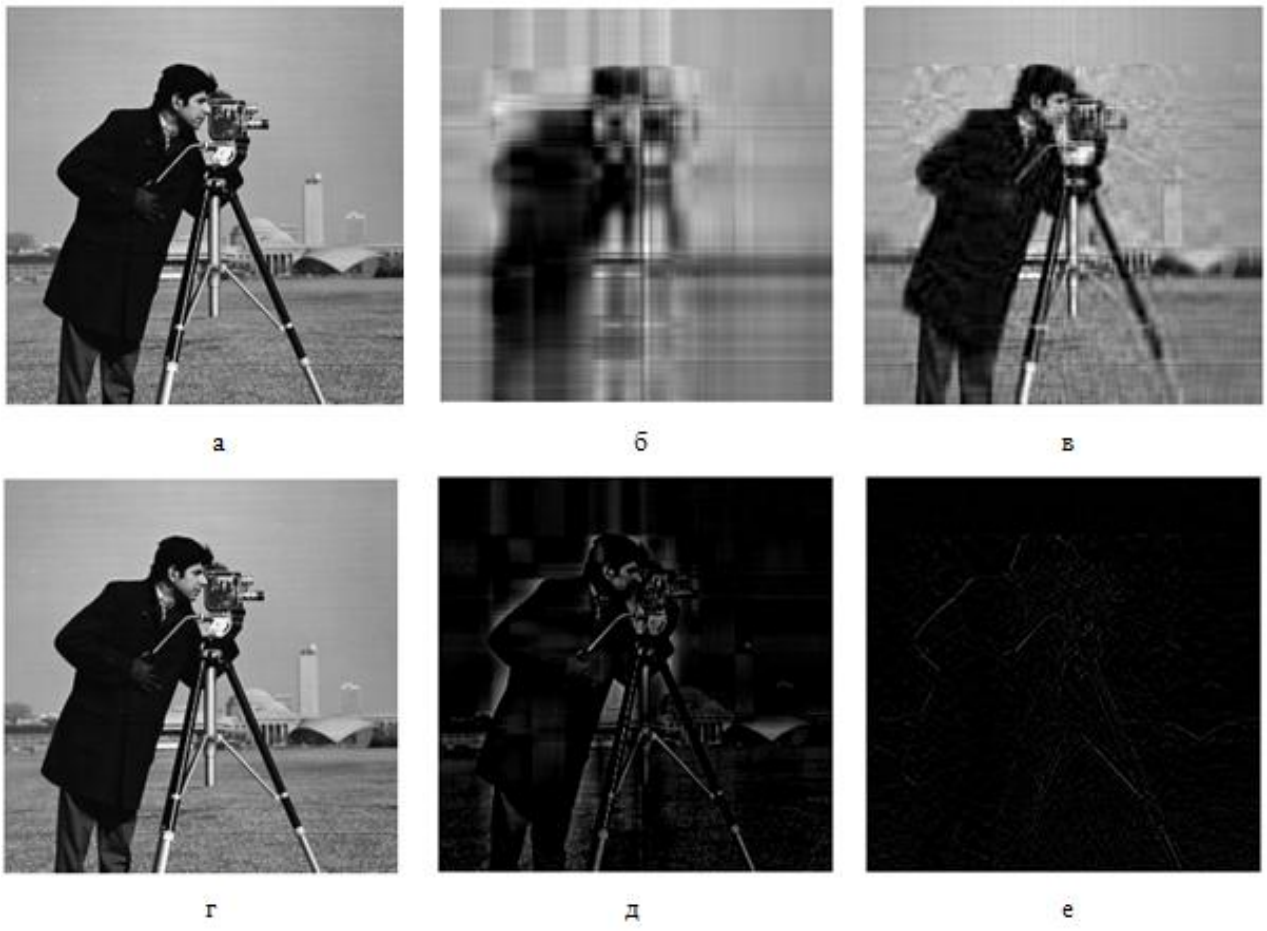


Рис.9.1. Зображення CAMERAMAN і його апроксимації: первісне зображення (а); F_5 (б); F_{20} (в); F_{150} (г); F_{5_d} (д); F_{40_d} (е)

Виходячи з розглянутих результатів, висувається гіпотеза: сингулярні трійки, що відповідають найбільшим СНЧ, відповідають головним чином низькочастотним, а найменшим - високочастотним складовим сигналу.

Для перевірки гіпотези в середовищі MATLAB був проведений обчислювальний експеримент, у якому використовувалися 1000 різних по розміру, яскравості, фактурі і т.д. зображень у градаціях сірого. Для наочності ілюстрації основних результатів розглянемо як вхідне зображення головну підматрицю WW матриці F зображення POUT розміру 11×11, що дає типову якісну картину. Будемо позначати матрицю центрованого енергетичного спектра довільної матриці A як $SPECTR\,(A)$. Розглянемо для WW центровані енергетичні спектри деяких її складових, апроксимацій і доповнень до апроксимацій (рис.9.2 — виділені найбільші й найменші значення спектральних коефіцієнтів). Як видне з наведених результатів, сингулярні трійки, що відповідають максимальним СНЧ, відповідають, головним чином, низькочастотним складовим сигналу-зображення. Разом із зменшенням СНЧ відбувається підключення середніх і високих частот, а внесок низьких стає усе менше. Найменші СНЧ відповідають високочастотним складовим двовимірного цифрового сигналу.

Перевіримо, як реагує енергетичний спектр вхідного зображення WW на збурення різних СНЧ. При проведенні обчислювального експерименту збурення найбільших СНЧ приводили до збурень у центральній частині матриці центрованого спектра, залишаючи практично незмінними високочастотні складові. При збуренні малих СНЧ, картина змінювалася на протилежну: значно збурювалися високочастотні складові енергетичного спектра й практично не зачіпалися інші частотні складові. Наприклад, якщо значення $\sigma_{10}=0.5704$ покласти рівним 0.0008, матриця відносних збурень (погрішностей) кожного елемента

центрованого енергетичного спектра, обчислених у відсотках, буде мати вигляд (жирним шрифтом виділені максимальні відносні погрішності):

23.6480	**4.4449**	**4.4375**	0.7313	0.9534	0.0026	0.1649	0.6653	0.0679	**15.8227**	**2.4734**
61.7384	**5.6856**	1.0781	1.2315	1.2946	0.0004	0.1883	1.3749	0.3244	**2.6020**	**5.8417**
2.8855	1.8952	1.1789	3.0755	0.1963	0.0002	0.1284	0.9665	0.2908	1.7989	**4.9052**
0.3363	0.1977	0.0943	0.0294	0.0042	0.0000	0.0073	0.0425	0.0405	0.1022	0.2421
1.8512	0.3385	0.0985	0.0669	0.0065	0.0000	0.0124	0.0950	0.1105	1.6317	2.2347
0.0000	0.0037	0.0018	0.0011	0.0002	0.0000	0.0002	0.0011	0.0018	0.0037	0.0000
2.2347	1.6317	0.1105	0.0950	0.0124	0.0000	0.0065	0.0669	0.0985	0.3385	1.8512
0.2421	0.1022	0.0405	0.0425	0.0073	0.0000	0.0042	0.0294	0.0943	0.1977	0.3363
4.9052	1.7989	0.2908	0.9665	0.1284	0.0002	0.1963	3.0755	1.1789	1.8952	**2.8855**
5.8417	**2.6020**	0.3244	1.3749	0.1883	0.0004	1.2946	1.2315	1.0781	**5.6856**	**61.7384**
2.4734	**15.8227**	0.0679	0.6653	0.1649	0.0026	0.9534	0.7313	**4.4375**	**4.4449**	**23.6480**

$SPECTR(S_1) =$

1.0e+004 *

0.0000	0.0000	0.0000	0.0000	0.0000	0.0015	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0024	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0001	0.0001	0.0072	0.0001	0.0001	0.0000	0.0000	0.0000
0.0001	0.0001	0.0001	0.0001	0.0003	**0.0136**	0.0003	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0002	**0.0161**	**0.0217**	**0.0161**	0.0002	0.0001	0.0001	0.0001
0.0060	0.0067	0.0082	0.0145	**0.0265**	**1.3294**	**0.0265**	0.0145	0.0082	0.0067	0.0060
0.0001	0.0001	0.0001	0.0002	**0.0161**	**0.0217**	**0.0161**	0.0002	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0003	**0.0136**	0.0003	0.0001	0.0001	0.0001	0.0001
0.0000	0.0000	0.0000	0.0001	0.0001	0.0072	0.0001	0.0001	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0024	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0015	0.0000	0.0000	0.0000	0.0000	0.0000

$SPECTR(S_4) =$

3.5943	10.1517	9.9107	10.4392	7.9704	0.2183	7.9704	10.4392	9.9107	10.1517	3.5943
2.1460	6.0612	5.9173	6.2328	4.7588	0.1304	4.7588	6.2328	5.9173	6.0612	2.1460
5.5889	15.7850	15.4103	16.2320	12.3933	0.3395	12.3933	16.2320	15.4103	15.7850	5.5889
8.8097	24.8817	24.2910	25.5863	19.5354	0.5351	19.5354	25.5863	24.2910	24.8817	8.8097
12.4076	35.0435	34.2116	36.0358	27.5137	0.7537	27.5137	36.0358	34.2116	35.0435	12.4076
0.0077	0.0218	0.0213	0.0224	0.0171	0.0005	0.0171	0.0224	0.0213	0.0218	0.0077
12.4076	35.0435	34.2116	36.0358	27.5137	0.7537	27.5137	36.0358	34.2116	35.0435	12.4076
8.8097	24.8817	24.2910	25.5863	19.5354	0.5351	19.5354	25.5863	24.2910	24.8817	8.8097
5.5889	15.7850	15.4103	16.2320	12.3933	0.3395	12.3933	16.2320	15.4103	15.7850	5.5889
2.1460	6.0612	5.9173	6.2328	4.7588	0.1304	4.7588	6.2328	5.9173	6.0612	2.1460
3.5943	10.1517	9.9107	10.4392	7.9704	0.2183	7.9704	10.4392	9.9107	10.1517	3.5943

$SPECTR(S_{10}) =$

1.8525	**1.1453**	0.5306	0.6668	0.1127	0.0007	0.1127	0.6668	0.5306	**1.1453**	**1.8525**
1.0079	0.6231	0.2887	0.3628	0.0613	0.0004	0.0613	0.3628	0.2887	0.6231	**1.0079**
1.2189	0.7536	0.3492	0.4387	0.0742	0.0005	0.0742	0.4387	0.3492	0.7536	**1.2189**
0.1168	0.0722	0.0335	0.0421	0.0071	0.0000	0.0071	0.0421	0.0335	0.0722	0.1168
0.4630	0.2863	0.1326	0.1667	0.0282	0.0002	0.0282	0.1667	0.1326	0.2863	0.4630
0.0119	0.0073	0.0034	0.0043	0.0007	0.0000	0.0007	0.0043	0.0034	0.0073	0.0119
0.4630	0.2863	0.1326	0.1667	0.0282	0.0002	0.0282	0.1667	0.1326	0.2863	0.4630
0.1168	0.0722	0.0335	0.0421	0.0071	0.0000	0.0071	0.0421	0.0335	0.0722	0.1168
1.2189	0.7536	0.3492	0.4387	0.0742	0.0005	0.0742	0.4387	0.3492	0.7536	**1.2189**
1.0079	0.6231	0.2887	0.3628	0.0613	0.0004	0.0613	0.3628	0.2887	0.6231	**1.0079**
1.8525	**1.1453**	0.5306	0.6668	0.1127	0.0007	0.1127	0.6668	0.5306	**1.1453**	**1.8525**

$SPECTR(WW_2) =$

1.0e+004 *

0.0000	**0.0002**	**0.0003**	**0.0007**	**0.0008**	0.0015	**0.0008**	**0.0006**	**0.0003**	**0.0002**	**0.0000**
0.0001	**0.0002**	**0.0004**	**0.0008**	0.0011	0.0024	0.0011	**0.0008**	**0.0004**	**0.0002**	**0.0000**
0.0001	**0.0005**	**0.0009**	0.0018	0.0023	0.0071	0.0023	0.0018	**0.0009**	**0.0004**	**0.0001**
0.0004	0.0015	0.0031	0.0062	0.0079	**0.0132**	0.0079	0.0062	0.0030	0.0015	**0.0003**
0.0008	0.0034	0.0070	**0.0142**	**0.0179**	**0.0206**	**0.0179**	**0.0142**	0.0070	0.0035	**0.0008**
0.0060	0.0067	0.0079	**0.0139**	**0.0257**	**1.3294**	**0.0257**	**0.0139**	0.0079	0.0067	0.0060
0.0008	0.0035	0.0070	**0.0142**	**0.0179**	**0.0206**	**0.0179**	**0.0142**	0.0070	0.0034	**0.0008**
0.0003	0.0015	0.0030	0.0062	0.0079	**0.0132**	0.0079	0.0062	0.0031	0.0015	**0.0004**
0.0001	**0.0004**	**0.0009**	0.0018	0.0023	0.0071	0.0023	0.0018	**0.0009**	**0.0005**	**0.0001**
0.0000	**0.0002**	**0.0004**	**0.0008**	0.0011	0.0024	0.0011	**0.0008**	**0.0004**	**0.0002**	**0.0001**
0.0000	**0.0002**	**0.0003**	**0.0006**	**0.0008**	0.0015	**0.0008**	**0.0007**	**0.0003**	**0.0002**	**0.0000**

$SPECTR(WW_{9d}) =$

1.8306	**1.3008**	**0.8762**	**0.7004**	0.2120	**0.0010**	0.1365	0.6360	**0.8354**	**0.9764**	**1.7938**
1.1550	**1.5701**	**0.7467**	0.5350	0.4071	**0.0006**	0.3099	0.2409	**0.6105**	**0.7124**	**0.9900**
1.3455	**1.8184**	**1.0021**	0.6491	0.4571	**0.0009**	0.3106	0.2299	0.8401	0.3811	**1.1132**
0.1548	0.5956	0.4820	**0.1032**	**0.2211**	**0.0005**	**0.2301**	**0.1549**	0.4931	0.6850	0.2113
0.4583	0.2072	**0.0930**	**0.1442**	**0.0358**	**0.0001**	**0.0786**	**0.1919**	**0.1471**	0.4248	0.4847
0.0118	**0.0072**	**0.0041**	**0.0043**	**0.0007**	**0.0000**	**0.0007**	**0.0043**	**0.0041**	**0.0072**	0.0118
0.4847	0.4248	**0.1471**	**0.1919**	**0.0786**	**0.0001**	**0.0358**	**0.1442**	**0.0930**	0.2072	0.4583
0.2113	0.6850	0.4931	**0.1549**	**0.2301**	**0.0005**	**0.2211**	**0.1032**	0.4820	0.5956	0.1548
1.1132	0.3811	0.8401	0.2299	0.3106	**0.0009**	0.4571	0.6491	**1.0021**	**1.8184**	**1.3455**
0.9900	**0.7124**	**0.6105**	0.2409	0.3099	**0.0006**	0.4071	0.5350	**0.7467**	**1.5701**	**1.1550**
1.7938	**0.9764**	**0.8354**	0.6360	0.1365	**0.0010**	0.2120	**0.7004**	**0.8762**	**1.3008**	**1.8306**

Рис.9.2. Матриці центрованих енергетичних спектрів

Таким чином, результати експерименту повністю підтвердили висунуту гіпотезу.

Враховуючи, що будь-яке СПр ОП еквівалентним чином представляється у вигляді збурень СНЧ і (або) СНВ матриці ОП, однозначно визначаємих нормальним SVD, зв'язок між енергетичним спектром сигналу й сингулярними трійками його матриці й той факт, що при вбудові ДІ в частотній області ОП для забезпечення стійкості стеганометоду до збурень і надійності сприйняття СП пріоритетної є модифікація середньої частини частотного спектра, можна зробити висновок, що аналогічними з погляду стійкості виявляться стеганометоди, для яких СПр збурить сингулярні трійки, що відповідають середнім за значенням сингулярним числам матриці ОП (відповідних до середньої частини частотного спектра контейнера), незалежно від безпосередньо використовуваної цими методами області вбудови ДІ.

Питання

1. Умови забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера.
2. Чому забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера є ключовим для забезпечення надійності спртйняття стеганоповідомлення?
3. Відповідність між параметрами двовимірного сигналу в частотній області ЦЗ та областях сингулярного, спектрального розкладання матриці.

Література

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
2. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.

Лекція 10. ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СПРИЙНЯТТЯ СТЕГАНОПОВІДОМЛЕННЯ (продовження)

План

1. Зв'язок перетворення Уолша-Адамара й дискретного косинусного перетворення
2. Зв'язок перетворення Уолша-Адамара й сингулярного розкладання матриці
3. Достатня умова забезпечення надійності сприйняття стеганоповідомлення в області перетворення Уолша-Адамара

1. Зв'язок перетворення Уолша-Адамара й дискретного косинусного перетворення

Завдяки високій обчислювальній ефективності, а також відповідності архітектурним особливостям сучасних процесорів, перспективними для сучасних СЗІ є стеганографічні методи, засновані на використанні простору перетворень Уолша-Адамара.

Дискретне перетворення Уолша-Адамара можна записати у вигляді наступного матричного добутку

$$V = YH_N, \tag{10.1}$$

де H_N — матриця Уолша-Адамара порядка $N = 2^k$, яка може бути побудована відповідно конструкції Сильвестра

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \tag{10.2}$$

де $H_1 = 1$, а Y — вектор-рядок довжини N.

Вираз (10.1) являє собою одномірне перетворення Уолша-Адамара. Для задач стеганографії, поширення отримало двовимірне дискретне перетворення Уолша-Адамара, яке визначається як

$$W = H'_N X H'^T_N, \tag{10.3}$$

де $H_N' = \frac{1}{\sqrt{N}} H_N$, а X — матриця розміру $N \times N$.

Між елементами матриці-результату перетворення Уолша-Адамара й частотними складовими матриці X існує певний зв'язок (рис.10.1). Найбільший інтерес для встановлення умови дотримання надійності сприйняття СП представляє локалізація образів високочастотних складових матриці X ЦЗ.

Кожна з функцій Уолша, не будучи гармонійною, характеризується частостю, яка є аналогом частоти для гармонійних функцій, і у випадку останніх ці дві характеристики співпадають. Якщо число змін знака в інтервалі часу функції $f(t)$ дорівнює η, то частость $\bar{\eta}$ функції f визначається як $\eta/2$ або $(\eta+1)/2$ при η парному чи непарному відповідно. Частость функції Уолша буде тим більше, чим більше частота відповідної гармоніки.

Позначимо $H_N(i,:)$ - і-ий рядок матриці H_N. У прийнятих позначеннях з урахуванням (10.2) відповідність між початковими рядками H_N і гармонійними функціями буде мати вигляд

$$H_N(1,:) \rightarrow sin(\pi t)$$
$$H_N(2,:) \rightarrow sin(N\pi t)$$

$$H_N(3,:) \rightarrow sin\left(\frac{N}{2}\pi t\right)$$
$$H_N(4,:) \rightarrow cos\left(\frac{N}{2}\pi t\right) \qquad (10.4)$$
……..,

і т.д.

Найбільшу частость серед рядків матриці (10.2) завжди буде мати $H_N(2,:)$, для якої $\overline{\eta} = N/2 = 2^{k-1}$; найбільшу частоту із усіх відповідних гармонік (10.4) має, гармоніка $sin(N\pi t)$, що відповідає $H_N(2,:)$

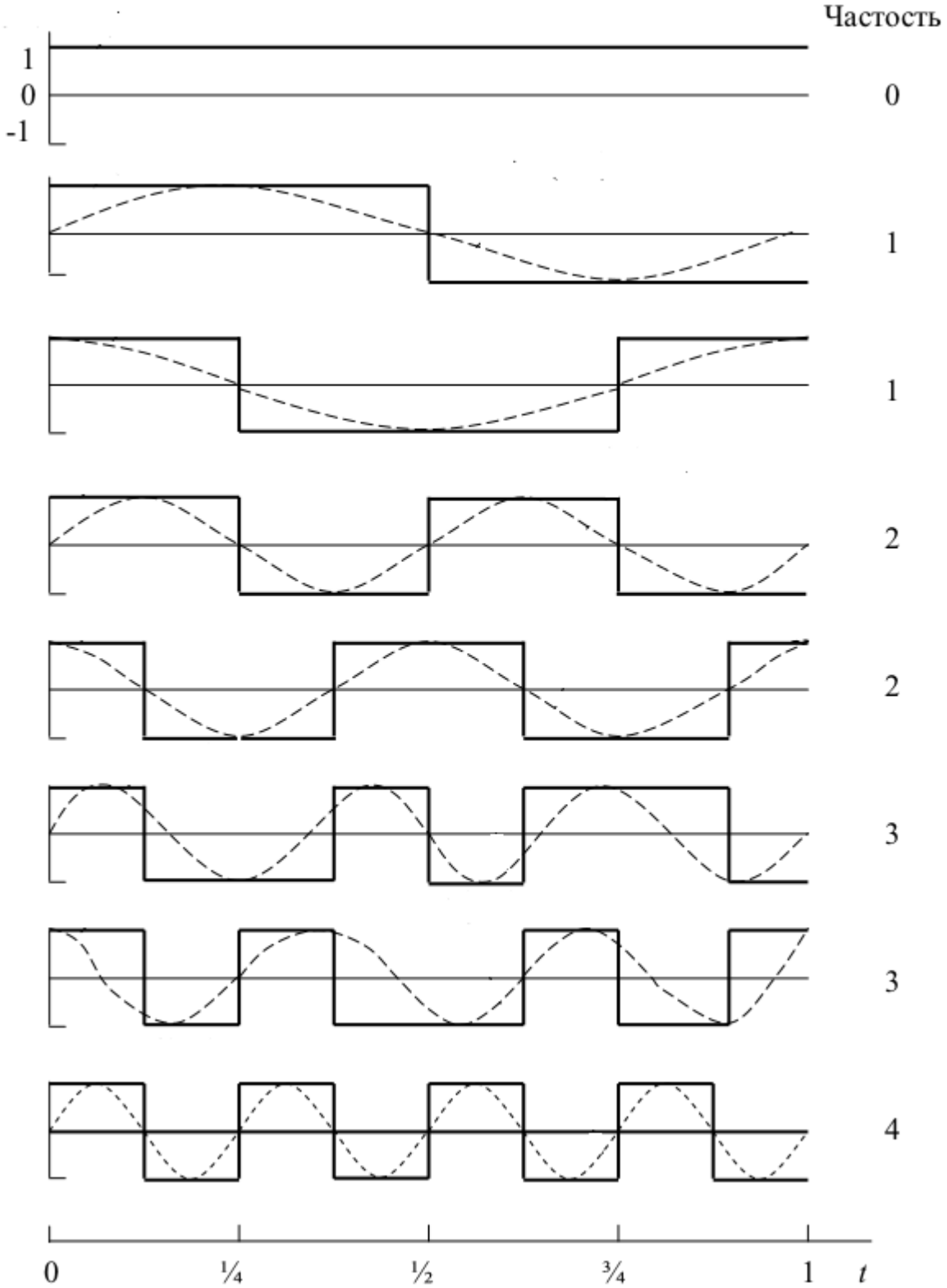


Рис.10.1. Відповідність між функціями Уолша (N=8) і гармоніками Фурьє

Для отримання зв’язку між частотними складовими й складовими перетвореної матриці Уолша-Адамара припустимо, що X=E, де E— одинична матриця відповідного розміру. У цьому випадку результат співвідношення (10.3) не буде ніяк залежати від матриці зображення, а буде визначатися тільки коефіцієнтами матриці Уолша-Адамара:

$$W = H'_N X H'^{T}_N = H'_N H'_N . \qquad (10.5)$$

Співвідношення (10.5) можна переписати у вигляді:

$$H'_N H'_N = \frac{1}{N}\begin{pmatrix} H_N(1,:) \\ H_N(2,:) \\ \ldots\ldots\ldots \\ H_N(N,:) \end{pmatrix} \cdot \left((H_N(1,:))^T, (H_N(2,:))^T, \ldots, (H_N(N,:))^T \right) =$$

$$= \frac{1}{N}\begin{pmatrix} H_N(1,:)(H_N(1,:))^T, & H_N(1,:)(H_N(2,:))^T, & \ldots, & H_N(1,:)(H_N(N,:))^T \\ H_N(2,:)(H_N(1,:))^T, & H_N(2,:)(H_N(2,:))^T, & \ldots, & H_N(2,:)(H_N(N,:))^T \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ H_N(N,:)(H_N(1,:))^T, & H_N(N,:)(H_N(2,:))^T, & \ldots, & H_N(N,:)(H_N(N,:))^T \end{pmatrix} \quad (10.6)$$

З урахуванням (10.6), відповідності (10.4) між функціями Уолша й відповідними гармоніками, а також відомих формул перетворення добутку тригонометричних функцій у суму, сформулюємо

Умову А: у матриці (10.3), що є результатом перетворення Уолша-Адамара, елемент (2,2) буде відповідати самій високочастотній складовій X, частина високочастотних складових буде локалізовано в межах 2 рядка й другого стовпця матриці (10.3), незалежно від її розміру. У межах другого рядка й другого стовпця низькочастотні складові відсутні. Взагалі ж у матрицях, що є результатом перетворення Уолша-Адамара, високочастотним складовим будуть відповідати елементи, що знаходяться на перетинанні рядків і стовпців, що відповідають дискретним функціям Уолша з найбільшими частостями. Таким чином, для локалізації елементів, що відповідають високочастотним складовим блоку (матриці) ЦЗ, достатньо серед функцій Уолша визначити функції з найбільшими частостями. Так з урахуванням частості дискретних функцій Уолша, використовуваних для перетворення матриць розміру $l \times l$, де $l \in \{4, 8, 16\}$, вказаних в табл. 10.1, можна стверджувати, що високочастотним складовим сигналу в матриці розміру 4×4 будуть відповідати в матриці (10.3) елементи, що знаходяться на позиціях (виписані в порядку спадання частоти): (2,2), (2,4) і (4,2); в матриці розміру 8×8: (2,2), (2,6) і (6,2), (2,8) і (6,8) і (6,6); в матриці розміру 16×16: (2,2), (2,10) і (10,2), (2,14) і (14,2), (2,6) і (6,2) і т.д. У порядку спадання частоти можна виписати всі елементи матриці, а не тільки ті, які відповідають високочастотним. Якщо частості функцій однакові, то при виявленні відповідності високочастотним складовим перевагу слід віддати тій, у якій більше значення η.

Таблиця 10.1. Відповідність між значеннями η і $\bar{\eta}$ для функцій Уолша для різних розмірів матриць Уолша-Адамара

l=4	Номер рядка	1		2		3		4	
	$\eta/\bar{\eta}$	0/0		3/2		1/1		2/1	
l=8	Номер рядка	1	2	3	4	5	6	7	8

	$\eta / \bar{\eta}$	0/0		7/4		3/2		4/2		1/1		6/3		2/1		5/3	
l=16	Номер рядка	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	$\eta / \bar{\eta}$	0/0	15/8	7/4	8/4	3/2	12/6	4/2	11/6	1/1	14/7	6/3	9/5	2/1	13/7	5/3	10/5

Отримані результати знайшли своє підтвердження на практиці (рис. 10.2 - локалізація високочастотних складових виділена жовтою заливкою відповідних елементів).

Таким чином, для матриці, що є результатом перетворення Уолша-Адамара матриці *X* довільного розміру, можна точно встановити елементи, що відповідають високочастотним складовим матриці *X*. СПр, результатом якого є збурення цих елементів в області перетворення Уолша-Адамара, забезпечить надійність сприйняття одержуваного СП.

(1,1)	(1,4)	(1,2)	(1,3)
(4,1)	(4,4)	(4,2)	(4,3)
(2,1)	(2,4)	(2,2)	(2,3)
(3,1)	(3,4)	(3,2)	(3,3)

а

(1,1)	(1,8)	(1,4)	(1,5)	(1,2)	(1,7)	(1,3)	(1,6)
(8,1)	(8,8)	(8,4)	(8,5)	(8,2)	(8,7)	(8,3)	(8,6)
(4,1)	(4,8)	(4,4)	(4,5)	(4,2)	(4,7)	(4,3)	(4,6)
(5,1)	(5,8)	(5,4)	(5,5)	(5,2)	(5,7)	(5,3)	(5,6)
(2,1)	(2,8)	(2,4)	(2,5)	(2,2)	(2,7)	(2,3)	(2,6)
(7,1)	(7,8)	(7,4)	(7,5)	(7,2)	(7,7)	(7,3)	(7,6)
(3,1)	(3,8)	(3,4)	(3,5)	(3,2)	(3,7)	(3,3)	(3,6)
(6,1)	(6,8)	(6,4)	(6,5)	(6,2)	(6,7)	(6,3)	(6,6)

б

(1,1)	(1,16)	(1,8)	(1,9)	(1,4)	(1,13)	(1,5)	(1,12)	(1,2)	(1,15)	(1,7)	(1,10)	(1,3)	(1,14)	(1,6)	(1,11)
(16,1)	(16,16)	(16,8)	(16,9)	(16,4)	(16,13)	(16,5)	(16,12)	(16,2)	(16,15)	(16,7)	(16,10)	(16,3)	(16,14)	(16,6)	(16,11)
(8,1)	(8,16)	(8,8)	(8,9)	(8,4)	(8,13)	(8,5)	(8,12)	(8,2)	(8,15)	(8,7)	(8,10)	(8,3)	(8,14)	(8,6)	(8,11)
(9,1)	(9,16)	(9,8)	(9,9)	(9,4)	(9,13)	(9,5)	(9,12)	(9,2)	(9,15)	(9,7)	(9,10)	(9,3)	(9,14)	(9,6)	(9,11)
(4,1)	(4,16)	(4,8)	(4,9)	(4,4)	(4,13)	(4,5)	(4,12)	(4,2)	(4,15)	(4,7)	(4,10)	(4,3)	(4,14)	(4,6)	(4,11)
(13,1)	(13,16)	(13,8)	(13,9)	(13,4)	(13,13)	(13,5)	(13,12)	(13,2)	(13,15)	(13,7)	(13,10)	(13,3)	(13,14)	(13,6)	(13,11)
(5,1)	(5,16)	(5,8)	(5,9)	(5,4)	(5,13)	(5,5)	(5,12)	(5,2)	(5,15)	(5,7)	(5,10)	(5,3)	(5,14)	(5,6)	(5,11)
(12,1)	(12,16)	(12,8)	(12,9)	(12,4)	(12,13)	(12,5)	(12,12)	(12,2)	(12,15)	(12,7)	(12,10)	(12,3)	(12,14)	(12,6)	(12,11)
(2,1)	(2,16)	(2,8)	(2,9)	(2,4)	(2,13)	(2,5)	(2,12)	(2,2)	(2,15)	(2,7)	(2,10)	(2,3)	(2,14)	(2,6)	(2,11)
(15,1)	(15,16)	(15,8)	(15,9)	(15,4)	(15,13)	(15,5)	(15,12)	(15,2)	(15,15)	(15,7)	(15,10)	(15,3)	(15,14)	(15,6)	(15,11)
(7,1)	(7,16)	(7,8)	(7,9)	(7,4)	(7,13)	(7,5)	(7,12)	(7,2)	(7,15)	(7,7)	(7,10)	(7,3)	(7,14)	(7,6)	(7,11)
(10,1)	(10,16)	(10,8)	(10,9)	(10,4)	(10,13)	(10,5)	(10,12)	(10,2)	(10,15)	(10,7)	(10,10)	(10,3)	(10,14)	(10,6)	(10,11)
(3,1)	(3,16)	(3,8)	(3,9)	(3,4)	(3,13)	(3,5)	(3,12)	(3,2)	(3,15)	(3,7)	(3,10)	(3,3)	(3,14)	(3,6)	(3,11)
(14,1)	(14,16)	(14,8)	(14,9)	(14,4)	(14,13)	(14,5)	(14,12)	(14,2)	(14,15)	(14,7)	(14,10)	(14,3)	(14,14)	(14,6)	(14,11)
(6,1)	(6,16)	(6,8)	(6,9)	(6,4)	(6,13)	(6,5)	(6,12)	(6,2)	(6,15)	(6,7)	(6,10)	(6,3)	(6,14)	(6,6)	(6,11)
(11,1)	(11,16)	(11,8)	(11,9)	(11,4)	(11,13)	(11,5)	(11,12)	(11,2)	(11,15)	(11,7)	(11,10)	(11,3)	(11,14)	(11,6)	(11,11)

в

Рис. 10.2. Відповідність трансформант УА коефіцієнтам ДКП для блоків різного розміру l×l: а – l=4; б – l=8; в – l=16;

2. Зв'язок перетворення Уолша-Адамара й сингулярного розкладання матриці

Формальні достатні умови забезпечення надійності сприйняття СП є в області спектрального розкладання симетричної матриці, сингулярного розкладання довільної матриці (див. «Методичні вказівки до лабораторних робіт»). Відповідно до останнього надійність сприйняття СП буде забезпечуватися в тому випадку, якщо СНВ (блоків) матриці, що збурені в результаті СПр, відповідають малим СНЧ або СНЧ, які мають малі відокремленості. При цьому, чим менше збурення СНЧ, відокремленості й значення СНЧ, які відповідають збуреним СНВ, тим більше ймовірність дотримання надійності сприйняття СП.

Нехай B – довільний $l \times l$-блок з отриманих шляхом стандартної розбивки блоків матриці F ЦЗ з СНЧ $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_l \geq 0$. В матриці ЦЗ:

$$\sigma_1 >> \sigma_2 \geq \ldots \geq \sigma_l \geq 0.$$

Відокремленість найменших за значенням СНЧ в (блоці) ЦЗ може бути значно менше одиниці (аж до порівнянності з 0), що приводить до того, що СНЧ, про яких мова йде в достатній умові, - це найменші за значенням СНЧ. Сингулярне розкладання матриці B розглянемо у формі зовнішніх добутків:

$$B = \sum_{i=1}^{l} \sigma_i u_i v_i^T, \qquad (10.7)$$

яка дає представлення B у вигляді суми матриць одиничного рангу, кожна з яких відповідає своїй сингулярній трійці (σ_i, u_i, v_i). З урахуванням цього згадану достатню умову можна сформулювати в трохи іншій формі: надійність сприйняття СП буде забезпечуватися в тому випадку, коли при формальному представленні СПр в області сингулярного розкладання блоків матриці це виразиться в збуренні в матрицях одиничного рангу, що відповідають найменшим за значенням СНЧ в (10.7).

У достатній умові, сформульованій в області сингулярного розкладання матриці, ми не маємо такого чіткого поділу по частотних складових, як в області ДКП або перетворення Фур'є, оскільки кожна сингулярна трійка (і відповідна їй однорангова матриця) несе в собі інформацію про всі частоти, але в різній мірі. Розподіл частот між сингулярними трійками більш «м'який», чим безпосередньо в частотній області, що дає свої переваги в стеганографії.

Відсутність чіткого розподілу на частоти приведе й до більш «м'якої» відповідності між сингулярними трійками матриці й елементами матриці-результату перетворення Уолша-Адамара, дасть можливість для «більшого маневру» у процесі СПр, не погіршуючи надійність сприйняття СП, розширюючи можливу область перетворення, підтвердженням чого є результати обчислювальний експерименту. Область можливого збурення блоків ЦЗ в області перетворення Уолша-Адамара, що дає можливість збереження надійності сприйняття СП, розширена (рис. 10.3). Отримана картина абсолютно природня. Додаткове розширення області можливого збурення без порушення надійності сприйняття відбувається, по суті, за рахунок підключення елементів, які можна віднести вже до таких, які відповідають середньочастотній складовій, яка, як відомо, зі значною ймовірністю не порушує надійність сприйняття.

(1,1)	(1,4)	(1,2)	(1,3)
(4,1)	(4,4)	(4,2)	(4,3)
(2,1)	(2,4)	(2,2)	(2,3)
(3,1)	(3,4)	(3,2)	(3,3)

а

(1,1)	(1,8)	(1,4)	(1,5)	(1,2)	(1,7)	(1,3)	(1,6)
(8,1)	(8,8)	(8,4)	(8,5)	(8,2)	(8,7)	(8,3)	(8,6)
(4,1)	(4,8)	(4,4)	(4,5)	(4,2)	(4,7)	(4,3)	(4,6)
(5,1)	(5,8)	(5,4)	(5,5)	(5,2)	(5,7)	(5,3)	(5,6)
(2,1)	(2,8)	(2,4)	(2,5)	(2,2)	(2,7)	(2,3)	(2,6)
(7,1)	(7,8)	(7,4)	(7,5)	(7,2)	(7,7)	(7,3)	(7,6)
(3,1)	(3,8)	(3,4)	(3,5)	(3,2)	(3,7)	(3,3)	(3,6)
(6,1)	(6,8)	(6,4)	(6,5)	(6,2)	(6,7)	(6,3)	(6,6)

б

(1,1)	(1,16)	(1,8)	(1,9)	(1,4)	(1,13)	(1,5)	(1,12)	(1,2)	(1,15)	(1,7)	(1,10)	(1,3)	(1,14)	(1,6)	(1,11)
(16,1)	(16,16)	(16,8)	(16,9)	(16,4)	(16,13)	(16,5)	(16,12)	(16,2)	(16,15)	(16,7)	(16,10)	(16,3)	(16,14)	(16,6)	(16,11)
(8,1)	(8,16)	(8,8)	(8,9)	(8,4)	(8,13)	(8,5)	(8,12)	(8,2)	(8,15)	(8,7)	(8,10)	(8,3)	(8,14)	(8,6)	(8,11)
(9,1)	(9,16)	(9,8)	(9,9)	(9,4)	(9,13)	(9,5)	(9,12)	(9,2)	(9,15)	(9,7)	(9,10)	(9,3)	(9,14)	(9,6)	(9,11)
(4,1)	(4,16)	(4,8)	(4,9)	(4,4)	(4,13)	(4,5)	(4,12)	(4,2)	(4,15)	(4,7)	(4,10)	(4,3)	(4,14)	(4,6)	(4,11)
(13,1)	(13,16)	(13,8)	(13,9)	(13,4)	(13,13)	(13,5)	(13,12)	(13,2)	(13,15)	(13,7)	(13,10)	(13,3)	(13,14)	(13,6)	(13,11)
(5,1)	(5,16)	(5,8)	(5,9)	(5,4)	(5,13)	(5,5)	(5,12)	(5,2)	(5,15)	(5,7)	(5,10)	(5,3)	(5,14)	(5,6)	(5,11)
(12,1)	(12,16)	(12,8)	(12,9)	(12,4)	(12,13)	(12,5)	(12,12)	(12,2)	(12,15)	(12,7)	(12,10)	(12,3)	(12,14)	(12,6)	(12,11)
(2,1)	(2,16)	(2,8)	(2,9)	(2,4)	(2,13)	(2,5)	(2,12)	(2,2)	(2,15)	(2,7)	(2,10)	(2,3)	(2,14)	(2,6)	(2,11)
(15,1)	(15,16)	(15,8)	(15,9)	(15,4)	(15,13)	(15,5)	(15,12)	(15,2)	(15,15)	(15,7)	(15,10)	(15,3)	(15,14)	(15,6)	(15,11)
(7,1)	(7,16)	(7,8)	(7,9)	(7,4)	(7,13)	(7,5)	(7,12)	(7,2)	(7,15)	(7,7)	(7,10)	(7,3)	(7,14)	(7,6)	(7,11)
(10,1)	(10,16)	(10,8)	(10,9)	(10,4)	(10,13)	(10,5)	(10,12)	(10,2)	(10,15)	(10,7)	(10,10)	(10,3)	(10,14)	(10,6)	(10,11)
(3,1)	(3,16)	(3,8)	(3,9)	(3,4)	(3,13)	(3,5)	(3,12)	(3,2)	(3,15)	(3,7)	(3,10)	(3,3)	(3,14)	(3,6)	(3,11)
(14,1)	(14,16)	(14,8)	(14,9)	(14,4)	(14,13)	(14,5)	(14,12)	(14,2)	(14,15)	(14,7)	(14,10)	(14,3)	(14,14)	(14,6)	(14,11)
(6,1)	(6,16)	(6,8)	(6,9)	(6,4)	(6,13)	(6,5)	(6,12)	(6,2)	(6,15)	(6,7)	(6,10)	(6,3)	(6,14)	(6,6)	(6,11)
(11,1)	(11,16)	(11,8)	(11,9)	(11,4)	(11,13)	(11,5)	(11,12)	(11,2)	(11,15)	(11,7)	(11,10)	(11,3)	(11,14)	(11,6)	(11,11)

в

Рис. 10.3. Локалізація області можливого збурення в результаті СПр в області перетворення Уолша-Адамара для l×l-блоків ЦЗ: а – l=4; б – l=8; в – l=16

3. Достатня умова забезпечення надійності сприйняття стеганоповідомлення в області перетворення Уолша-Адамара

Достатня умова забезпечення надійності сприйняття стеганоповідомлення. Для забезпечення надійності сприйняття СП достатньо проводити вбудову додаткової інформації таким чином, щоб в області перетворення Уолша-Адамара його результатом було збурення елементів, локалізація яких наведена на рис. 10.3 для $l \times l$-блоків розміру $l \in \{4,8,16\}$, при цьому сама вбудова ДІ може здійснюватися не тільки безпосередньо в області Уолша-Адамара, а й у будь-якій іншій області контейнера (просторовій, області перетворення). При необхідності використання блоків іншого розміру рекомендується проводити вбудову ДІ таким чином, щоб результатом її було збурення елементів в області перетворення Уолша-Адамара в межах другого стовпця й другого рядка перетвореної матриці. Для більш точної локалізації можливих збурень необхідно провести додаткові дослідження з урахуванням умови А.

Отримана достатня умова знайшла своє підтвердження на практиці (табл. 10.2).

Таблица 10.2

Возмущенные элементы блока в области преобразования Уолша-Адамара	(2,2)	(2,6)&(6,2)	(2,8)/(8,2)	(2,4)&(4,2)	(2,2)&(2,8)&(8,2)&(2,6)& &(6,2)&(2,4)&(4,2)	(6,6)	(8,8)	(6,6)& (6,8)&(8,6)&(8,8)	(2,2)&(2,8)&(8,2)&(2,6)& &(6,2)&(2,4)&(4,2)& &(6,6)& (6,8)&(8,6)& &(8,8)
PSNR (*dB*)	48.1	45.2	45.1	45.1	39.7	48.0	48.0	42.1	37.7

Питання

1. Яке матричне перетворення називається перетворення Уолша_Адамара? Переваги такого перетвореня.

2. Зв'язок перетворення Уолша-Адамара й дискретного косинусного перетворення.
3. Зв'язок перетворення Уолша-Адамара й сингулярного розкладання матриці.
4. Достатня умова забезпечення надійності сприйняття стеганоповідомлення в області перетворення Уолша-Адамара. Як ця достатня умова повязана з аналогічними, але в інших областях ЦЗ?

Література

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
2. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.

Лекція 11. ЧУТЛИВІСТЬ СТЕГАНОПОВІДОМЛЕННЯ ДО ЗБУРНИХ ДІЙ

План

1. Умова нечутливості стеганоповідомлення до збурних дій
2. Кількісна оцінка захищеності стеганоповідомлення

1. Умова нечутливості стеганоповідомлення до збурних дій

Одна з основних вимог, що висуваються до будь-якого СП із метою забезпечення ефективного декодування секретної інформації, - нечутливість до збурних дій.

Визначення. СП будемо називати чутливим, якщо навіть незначні збурні дії, яких воно зазнає, здатні зруйнувати значну частину вбудованої ДІ й привести до виникнення великої кількості помилок при декодуванні ДІ, і нечутливим інакше.

Скрізь нижче розглядаються такі збурення, що впливають на ОП і СП, які забезпечують високу ймовірність забезпечення надійності сприйняття, - малі збурні дії.

Серед стеганоалгоритмів приховання даних у ЦЗ найбільш популярними є узагальнені групи методів, що працюють у просторовій і частотній областях. Більш стійкими до різноманітних спотворень вважаються методи другої групи, що апріорі забезпечує «програшну» з погляду стійкості позицію стеганоалгоритмам із першої групи, хоча використання області первинного зображення, що не вимагає яких-небудь додаткових витрат для побудови різних його перетворень, в обчислювальному сенсі є більш привабливим.

Однак, з огляду на попередні лекції, на основі теорії збурень отримані результати які говорять про те, що стійкість стеганоалгоритмів до збурних дій, як і інші властивості, визначається не використовуваною областю вбудови ДІ, а локалізацією збурень СНЧ (ВЗ) і СНВ (ВВ), що відбулися в результаті СПр ОП.

Нехай F — матриця контейнера.

Визначення. Стеганоалгоритм назвемо нестійким, якщо малі збурні дії можуть привести до значного або повного знищенню вбудованої в контейнер за допомогою цього алгоритму секретної інформації, і стійким інакше.

Таким чином, стеганоалгоритм буде нестійким, якщо згенероване їм СП буде чутливим до збурень.

Нехай СПр, що здійснюється деяким стеганоалгоритмом, збурило СНВ матриці ОП. Достатньою умовою забезпечення малої чутливості одержуваного СП до збурень, а тому стійкості використовуваного стеганоалгоритму, незалежно від області вбудови ДІ (просторової або області якого-небудь перетворення), є відповідність збурених СНВ сингулярним числам з великою відокремленістю. Відокремленість СНЧ, що відповідають збуреним СНВ матриці ОП, є мірою чутливості отриманого СП до збурних дій.

Наслідком з цього є наступне. Нехай $\overline{F}$ — матриця СП, результатом СПр є збурення матриці СНВ U, що отримана нормальним SVD матриці ОП F. Якщо збурення U відповідає СНВ, що відповідають СНЧ із малою відокремленістю, то одержуване СП виявиться чутливим до збурних дій, незалежно від самого алгоритму й використовуваної області вбудови ДІ.

Нехай тепер A — довільна симетрична матриця, що розглядається як матриця контейнера. Матриці СП $\overline{A}$ і довільної збурної дії E будуть розглядатися як симетричні (див.лекцію 1-2). Для оцінки чутливості СП тут має сенс аналізувати збурення тільки ВВ при СПр матриці ОП, а ДІ представляти у вигляді сукупності цих збурень (див.лекцію 1-2).

Достатньою умовою забезпечення малої чутливості СП до збурних дій є відповідність збурених при СПр власних векторів ОП власним значенням матриці СП, що мають великі абсолютні відокремленості.

Доказ. При СПр деякі (всі) ВВ матриці A ОП збуряться, відхилившись від первісного положення на деякі кути. Це відбудеться завжди, якщо тільки алгоритм вбудови ДІ не базується на безпосередній модифікації лише ВЗ матриці контейнера. Сукупність збурень ВВ є формальним представленням для ДІ. Таким чином, чутливість отриманого СП буде

визначатися чутливістю збурених при СПр ВВ матриці A. Очевидно, щоб зберегти незмінною вбудовану ДІ при збурній дії на СП, відхилення ВВ, що виникли в результаті СПр, повинні залишитися незмінними.

Нормальне спектральне розкладання (СР) матриці СП $\overline{A}$ представляється в вигляді (див.лекцію 1-2): $\overline{A}=\overline{U}\overline{\Lambda}\overline{U}^{T}$. Нехай E — матриця збурення $\overline{A}$. Тоді нормальне СР симетричної матриці $\overline{A}+E$ визначається як $\overline{A}+E=\overline{\overline{U}}\overline{\overline{\Lambda}}\overline{\overline{U}}^{T}$. Нехай $\overline{u}_i, \overline{\overline{u}}_i$ — нормовані ВВ $\overline{A}$ і $\overline{A}+E$ відповідно, що відповідають $i-му$ ВЗ, а θ_i — кут між ними. Збурені при СПр контейнера ВВ, а значить і стеганоповідомлення у цілому, будуть нечутливими до збурних дій, якщо відповідні ВЗ матриці $\overline{A}$ мають великі абсолютні відокремленості, причому, чим більше $gap_{abs}(i,\overline{A})$, тим менш чутливим до збурень буде відповідний ВВ. Таким чином, абсолютні відокремленості ВЗ, що відповідають збуреним при стеганоперетворенні ВВ, визначають чутливість отриманого СП. СП буде найменш чутливим до збурних дій, якщо СПр збурить ВВ матриці ОП, що відповідають ВЗ матриці СП, що мають найбільші абсолютні відокремленості. Більше того, як показує обчислювальний експеримент, найбільші абсолютні відокремленості ВЗ, присутніх у спектрі матриці СП, такі, що вони забезпечують нечутливість СП у зазначеному випадку (кути повороту відповідних ВВ становлять, часто, частки градусу).

Наслідок 1. Якщо збурені в результаті стеганоперетвоення ОП ВВ відповідають ВЗ матриці СП із малими абсолютними відокремленостями, то отримане СП виявляється чутливим до збурних дій, що, як правило, приводить до недостатньої ефективності декодування ДІ.

Враховуючи що всі збурення, що впливають на ОП і СП, є малими, абсолютні відокремленості ВЗ матриць $\overline{A}$ і A незначно відрізняються друг від друга. Звідки випливає

Наслідок 2. Достатньою умовою забезпечення малої чутливості СП до збурень є відповідність збурених при стеганоперетворенні контейнера ВВ власним значенням матриці ОП, що мають великі абсолютні відокремленості.

Из всего вышесказанного следует истинность следующего утверждения.

Чутливість СП до збурних дій у випадку симетричної матриці визначається чутливістю збурених ВВ матриці ОП при СПр. Виходячи зі значень збурень ВВ і абсолютних відокремленостей відповідних ВЗ можливо зробити якісні апріорні оцінки чутливості СП до збурних дій.

Якщо матриця ЦЗ-контейнера має довільну структуру, то в якості повного набору формальних параметрів може розглядатися набір СНЧ і СНВ матриці. Тоді можна стверджувати, що чутливість СП до збурних дій визначається чутливістю збурених СНВ матриці ОП при СПр. Виходячи зі значень збурень СНВ і відокремленостей відповідних СНЧ можливо зробити якісні апріорні оцінки чутливості СП до збурних дій.

Розглянемо один з стеганоалгоритмів, що задовольняє достатній умові нечутливості отримуваного стеганоповідомлення у випадку довільної матриці контейнера.

Вбудова ДІ

Крок 1. Матриця F розміром $n\times n$ ОП розбивається стандартним чином на $8\times 8-$блоки; B — довільний блок.

Крок 2. Нехай B - черговий блок контейнеру, що задіяний в процесі вбудови ДІ; p_i - черговий біт ДІ, що вбудовується в блок В:

2.1. Для B будується нормальне сингулярне розкладання: $B = U\Sigma V^T$; u_1 і v_1 — лівий і правий СНВ блока B відповідно, що відповідають максимальному СНЧ σ_1.

2.2. (вбудова p_i):

Якщо $p_i = 1$,

то

2.2.1. $\bar{u}_1 = n^O$, де $\bar{u}_1$ — збурений в результаті СПр u_1;

2.2.2. Обчислення $\bar{u}_2$,..., $\bar{u}_8$ — збурених $u_2,\ldots,u_8$ в процесі приведення лівих сингулярних векторів до ортонормованого з $\bar{u}_1$ виду шляхом розв'язку системи лінійних алгебраїчних рівнянь щодо елементів $\bar{u}_2$,..., $\bar{u}_8$;

інакше

2.2.1. $\bar{v}_1 = n^O$, де $\bar{v}_1$ — збурений в результаті СПр v_1;

2.2.2. Обчислення $\bar{v}_2$,..., $\bar{v}_8$ — збурених $v_2,\ldots,v_8$ в процесі приведення правих сингулярних векторів до ортонормованого з $\bar{v}_1$ виду шляхом розв'язку системи лінійних алгебраїчних рівнянь щодо елементів $\bar{v}_2$,..., $\bar{v}_8$.

2.3. (формування блоку $\bar{B}$ СП, що відповідає блоку B контейнера).

Якщо $p_i = 1$,

то $\bar{B} = \bar{U}\Sigma V^T$, де $\bar{U} = (n^O, \bar{u}_2, \ldots, \bar{u}_8)$

інакше $\bar{B} = U\Sigma \bar{V}^T$, де $\bar{V} = (n^O, \bar{v}_2, \ldots, \bar{v}_8)$.

Декодування ДІ.

Крок 1. Матриця СП $\bar{F}$ розміром $n \times n$ розбивається стандартним чином на $8 \times 8-$блоки; $\bar{B}$ — довільний блок.

Крок 2. З чергового блоку $\bar{B}$, що був задіяний при СПр, декодується черговий біт $\bar{p}_i$ ДІ:

2.1. Для $\bar{B}$ будується нормальне сингулярне розкладання: $\bar{B} = \bar{U}\bar{\Sigma}\bar{V}^T$; $\bar{u}_1$ і $\bar{v}_1$ — лівий і правий СНВ блока $\bar{B}$, що відповідають максимальному СНЧ $\bar{\sigma}_1$.

2.2. (декодування $\bar{p}_i$). Знайти $UN_в$ і $VN_в$ — кути між векторами $\bar{u}_1$, n^O і $\bar{v}_1$, n^O відповідно.

Якщо $UN_в < VN_в$,

то $\bar{p}_i = 1$,

інакше $\bar{p}_i = 0$.

Организация действий шага 2.2.2 при погружении ДИ может проводиться следующим образом (рассмотрим на примере матрицы U (рис.11.1), где u_i^O — вектор-столбец, ортогональный векторам $\bar{u}_1$ и $u_j^O, j = 2,..,i-1$). Обеспечение ортогональности левых СНВ

достигается путем решения системы из 28 линейных алгебраических уравнений с неизвестными $x_i, i = \overline{1,28}$ — элементами векторов u_i^o (рис.11.1):

$$\begin{cases} \left(\bar{u}_1, u_j^o\right) = 0,\ j = 2,..8, \\ \left(u_i^o, u_j^o\right) = 0, i = 2,..8,\ j = 2,..i-1, \end{cases}$$

где $(\bullet,\bullet)$ — скалярное произведение векторов-аргуметов. Матрица $\bar{U}$, фигурирующая при формировании матрицы $\bar{B}$ блока СС на шаге 2.3 при погружении дополнительной информации, включает в себя нормализованные векторы-столбцы $\frac{u_j^o}{\|u_j^o\|}, j = 2,..8$:

$$\bar{U} = \left(\bar{u}_1 \quad \frac{u_2^o}{\|u_2^o\|} \quad \frac{u_3^o}{\|u_3^o\|} \quad \dots \quad \frac{u_8^o}{\|u_8^o\|} \right) = (n^o, \bar{u}_2, ..., \bar{u}_8).$$

$$\begin{array}{c} \bar{u}_1 = n^o \quad u_2^o \quad u_3^o \quad u_4^o \quad u_5^o \quad u_6^o \quad u_7^o \quad u_8^o \\ \downarrow \quad\quad \downarrow \quad\quad \downarrow \quad\quad \downarrow \quad\quad \downarrow \quad\quad \downarrow \quad\quad \downarrow \quad\quad \downarrow \quad\quad \downarrow \end{array}$$

$$\begin{pmatrix} 1/\sqrt{8} & u_{12} & u_{13} & u_{14} & u_{15} & u_{16} & u_{17} & u_{18} \\ 1/\sqrt{8} & u_{22} & u_{23} & u_{24} & u_{25} & u_{26} & u_{27} & x_{22} \\ 1/\sqrt{8} & u_{32} & u_{33} & u_{34} & u_{35} & u_{36} & x_{16} & x_{23} \\ 1/\sqrt{8} & u_{42} & u_{43} & u_{44} & u_{45} & x_{11} & x_{17} & x_{24} \\ 1/\sqrt{8} & u_{52} & u_{53} & u_{54} & x_7 & x_{12} & x_{18} & x_{25} \\ 1/\sqrt{8} & u_{62} & u_{63} & x_4 & x_8 & x_{13} & x_{19} & x_{26} \\ 1/\sqrt{8} & u_{72} & x_2 & x_5 & x_9 & x_{14} & x_{20} & x_{27} \\ 1/\sqrt{8} & x_1 & x_3 & x_6 & x_{10} & x_{15} & x_{21} & x_{28} \end{pmatrix}$$

Рис.11.1. Збурена в процесі СПр матриця U

Ефективність СА оцінюється за допомогою коефіцієнта кореляції для ДІ:

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

де $p_i' = 1$, $\bar{p}_i' = 1$, якщо $p_i = 1$, $\bar{p}_i = 1$, и $p_i' = -1$, $\bar{p}_i' = -1$, якщо $p_i = 0$, $\bar{p}_i = 0$ (табл.11.1) .

Таблиця 11.1

Значення NC при атаці стиском з різними коефіцієнтами якості на стеганоповідомлення

QF (JPEG)	10	20	25	30	40	50	60	70	75	80	90
NC	0.94	0.95	0.95	0.95	0.95	0.95	0.95	0.96	0.96	0.96	0.96

2. Кількісна оцінка захищеності стеганоповідомлення

Для отримання кількісної оцінки чутливості СП повернемося до співвідношень (1.10), (1.11) (див. лекцію 1-2). Якщо

$$\|E\|_2 \geq \frac{gap_{abs}(i,\overline{A})}{2},$$

то оцінка збурення ВВ набуває вид

$$sin\,\theta_i \leq 1,$$

перетворюючись у тривіальну, і зробити висновок про реальну чутливість такого вектора не представляється можливим. Крім того, у цій ситуації в загальному випадку для θ_i принципово не можна знайти хоч якоїсь практичної оцінки. Дійсно, якщо збурення E настільки велике, то ВЗ матриці $\overline{A}+E$ може, достатньо віддалившись від ВЗ $\overline{A}$, стати кратним. Наприклад, $\overline{A}=diag(1.5,0.5)$, а $\overline{A}+E=I$. Оскільки будь-який ненульовий вектор розмірності 2 є ВВ для $\overline{A}+E$, то немає ніякої принципової можливості оцінити кут θ_i.

Визначення. Будемо казати, що ВЗ λ_i має достатню (недостатню) абсолютну відокремленість стосовно збурення E, якщо

$$\|E\|_2 < \frac{gap_{abs}(i,\overline{A})}{2} \quad \left(\|E\|_2 \geq \frac{gap_{abs}(i,\overline{A})}{2}\right).$$

Визначення. ВВ, які відповідають ВЗ із достатньою (недостатньою) абсолютною відокремленістю стосовно збурення E, назвемо захищеними (незахищеними) від розглянутого збурення.

Визначення. ДІ, результатом вбудови якої є збурення захищених ВВ, будемо називати додатковою інформацією, захищеною від збурення E (ЗІ).

Будемо вважати, що при збільшенні величини кута відхилення ВВ при СПр, збільшується й кількість ДІ, яка зберігається в збуренні цього вектора.

Зі зробленого припущення випливає, що СП тим менш чутливо, чим більшому збуренню при СПр піддалися ВВ, що відповідають ВЗ із максимальними абсолютними відокремленостями, чим більша «частина» ДІ є захищеною від збурних дій.

Кількісною оцінкою чутливості СП будемо вважати обсяг захищеної в ньому ДІ, що визначається з урахуванням збурень захищених ВВ і абсолютних відокремленостей відповідних ВЗ, безпосереднє обчислення якого розглянуто в наступній лекції.

Питання

1. Яке стеганоповідомлення називається чутливим?

2. Який стеганоалгоритм називається стійким/нестійким до збурних дій?
3. Достатня умова забезпечення малої чутливості СП до збурень.
4. Чим визначається чутливість СП до збурних дій у випадку симетричної матриці?
5. Коли ВЗ λ_i має достатню (недостатню) абсолютну відокремленість стосовно збурення E?
6. Які ВВ називаються захищеними (незахищеними) від збурення Е?

Література

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
2. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.

Лекція 12. ЧУТЛИВІСТЬ СТЕГАНОПОВІДОМЛЕННЯ ДО ЗБУРНИХ ДІЙ (продовження)

План

1. Метод порівняльної оцінки чутливості стеганоповідомлень до збурних дій
2. Оцінка ефективності методу порівняльної оцінки чутливості стеганоповідомлень до збурних дій

1. Метод порівняльної оцінки чутливості стеганоповідомлень до збурних дій

Пропонований метод порівняльної оцінки чутливості різних СП до збурних дій демонструється при розв'язку задачі про вибір ОП із заданої скінченної множини контейнерів для заданого секретного повідомлення з метою забезпечення найменшої чутливості одержуваного СП. При обчисленні обсягу ЗІ враховуються збурення ВВ при СПр і абсолютні відокремленості відповідних ВЗ, розглянуті в якості вагових коефіцієнтів.

Нехай $A_1, A_2, \ldots, A_k$ — симетричні матриці контейнерів розміру $n \times n$; $\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_k$ — відповідні матриці СП, отримані після вбудови в $A_1, A_2, \ldots, A_k$ однакового секретного повідомлення з використанням одного стеганоалгоритму.

Основні кроки методу представлені на рис.12.1.

Крок 1. Побудувати нормальні СР: $A_j = U_j \Lambda_j U_j^T$, $\overline{A}_j = \overline{U}_j \overline{\Lambda}_j \overline{U}_j^T$, $j = \overline{1,k}$;

Крок 2. Для $j = 1,2,\ldots k$:

а) Побудувати $\overline{VES_j}(i) = gap_{ab_3}(i, \overline{A}_j)$; $VES_j(i) = \dfrac{\overline{VES_j}(i)}{\left\|\overline{VES_j}\right\|}$, $i = \overline{1,n}$;

б) Побудувати $\overline{OTKLONENIYE_j}(i) = \sin \theta_i^{(j)}$, де $\theta_i^{(j)}$ — кут між $u_i(A_j)$ і $u_i(\overline{A}_j)$,

$OTKLONENIYE_j(i) = \dfrac{\overline{OTKLONENIYE_j}(i)}{\left\|\overline{OTKLONENIYE_j}\right\|}$, $i = \overline{1,n}$;

в) Побудувати вектор INF_j розподілу ДІ по ВВ СП:

$\overline{INF}_j(i) = VES_j(i) * OTKLONENIYE_j(i)$; $INF_j(i) = \dfrac{\overline{INF}_j(i)}{\sum_{i=1}^{n} \overline{INF}_j(i)} * 100\%$, $i = \overline{1,n}$;

г) Визначення ВЗ $\overline{\lambda}_{t_1}^{(j)}, \ldots, \overline{\lambda}_{t_p}^{(j)}$ СП $\overline{A}_j$ з достатньою абсолютною відокремленістю по відношенню до збурення E з використанням вектора $\overline{VES}_j$; визначення захищених ВВ;

д) Визначення обсягу захищеної інформації в СП $\overline{A}_j$: $OBYOM(j) = \sum_{i=1}^{p} INF_j(t_i)$;

Крок 3. Визначення СП з найбільшим обсягом ЗІ: $OBYOM(m) = \max_{1 \le j \le k} OBYOM(j)$;

A_m — шуканий контейнер

Рис.12.1. Алгоритм вибору ОП, що забезпечує найменшу чутливість СП

Зауваження. Нехай є деяке ОП, яке попередньо піддається стандартній розбивці на блоки фіксованого малого розміру. Запропонований метод може бути застосований до множини блоків контейнера, що дасть можливість для вибору блоків, які дадуть найменш чутливі блоки СП, і вбудову ДІ робити саме в ці блоки.

2. Оцінка ефективності методу порівняльної оцінки чутливості стеганоповідомлень до збурних дій

У реальних наборах операцій більшість задач обчислювальної математики, у тому числі й задача побудови спектрального розкладання матриці, є задачами необмеженої обчислювальної складності, тобто вирішуються приблизно. Якість наближеного розв'язку характеризується погрішністю, складовою частиною якої є обчислювальна погрішність. При реалізації на ЕОМ будь-якого алгоритму на його остаточний результат буде впливати (істотно чи ні) наявність помилок округлення. Цей факт не враховувався вище в пропонованому методі оцінки чутливості СП до збурних дій, основні обчислювальні витрати якого пов'язані з одержанням нормального СР матриць. Для оцінки сумарного впливу помилок округлення при обчисленні нормального СР на підсумкові результати роботи запропонованого методу використовується підхід, називаний зворотним аналізом помилок. При такому підході ВЗ і ВВ, отримані при чисельній реалізації нормального СР матриці A, що несуть в собі погрішність округлень, будемо розглядати як отримані точно, але для $A+H$ (задача зі збуреними вхідними даними) для деякої матриці H. Норма H задовольняє співвідношенню:

$$\|H\|_2 \le f(n)\varepsilon\|A\|_2, \qquad (12.1)$$

де n — розмір матриці A, $f(n)$ — функція розміру матриці, залежна від деталей обраного обчислювального методу, ε — одинична помилка округлення (roundoff error). У кожному разі оцінку (12.1) можна замінити на

$$\|H\|_2 < n\varepsilon\|A\|_2. \qquad (12.2)$$

Из (12.2) випливає, що H можна розглядати як мале збурення A, $\|H\|_2$ мала навіть при достатньо великому n (в обчислювальному експерименті, проведеному в середовищі Matlab, де $\varepsilon \approx 2.22e-16$, результати якого наведені нижче, $\|H\|_2 << 1$). Це означає, що, у силу нечутливості ВЗ, отриманий спектр лише дуже незначно буде відрізнятися від точних ВЗ матриці A, у силу чого якісна картина для абсолютних відокремленостей ВЗ, а тому й чутливостей відповідних ВВ не постраждає. Однак відреагують ВВ на збурну дію H відповідно до їхньої різної чутливості по-різному: найбільше від точних ВВ матриці A можуть відрізнятися отримані в результаті обчислень ВВ, які відповідають ВЗ із малими абсолютними відокремленостями. Однак збурення навіть чутливих ВВ будуть незначними в силу малості $\|H\|_2$, хоча й внесуть свій внесок в остаточний результат роботи алгоритму, запропонованого вище: в елементах вектора $OTKLONENIYE_j$ збурень ВВ при СПр контейнера A_j, що отримується на кроці 2,б(рис.12.1), складовою частиною очевидно будуть і помилки округлень. Помилки округлення, «розчиняючись» у підсумковому збуренні ВВ при СПр, «псують» якісну картину аналізу чутливості СП дуже незначно, підтвердженням чому є результати обчислювального експерименту. Таким чином, для тих контейнерів, розмір і норма матриці яких забезпечують малість правої частини (12.2), погрішностями округлень у запропонованому методі оцінки чутливості СП до збурних дій можна знехтувати.

Для ілюстрації отриманих результатів наведені результати обчислювального експерименту для ЦЗ в градаціях сірого однакового розміру (100×100),різних по контрастності, текстурі, жанру, за обсягом захищеної інформації. Для СПр були використані два стеганометоди, що здійснюють вбудову й декодування ДІ в різних областях: метод квантування зображень (просторова область) і метод відносної заміни величин коефіцієнтів

ДКП (частотна область). Випадковим чином генерувалося бінарне секретне повідомлення, однакове для всіх контейнерів, після вбудови якого на кожне СП накладався однаковий адитивний гауссовський шум, після чого проводилося декодування ДІ з збурених стеганоповідомлень. Результати проведених експериментів представлені на рис.12.2, 12.3, де обсяг відновленої при декодуванні інформації визначається як

$$P = \frac{Кількість\ біт\ секретного\ повідомлення, що\ декодовані\ вірно}{довжина\ секретного\ повідомлення} * 100\%$$

(крива ковзного усереднення будується з використанням 5 значень і наведена для більшої наочності результатів).

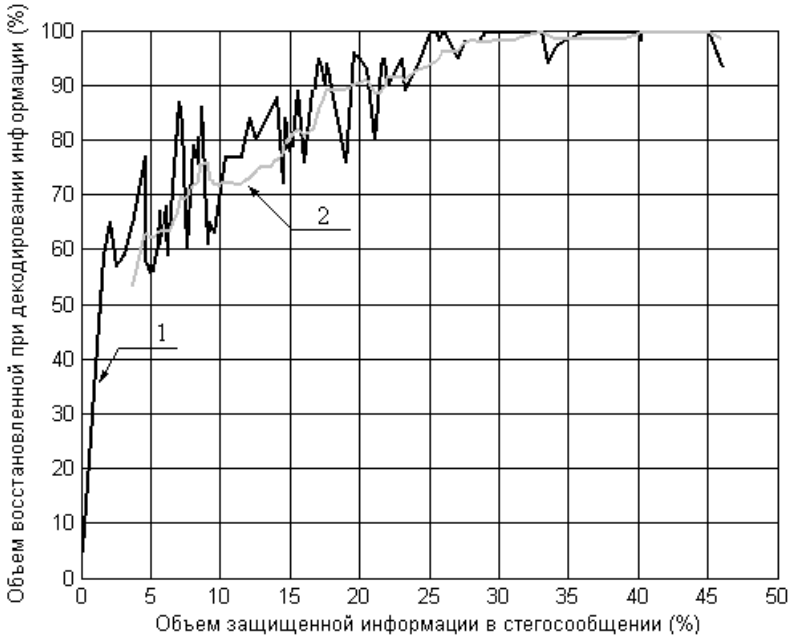


Рис.12.2. Метод квантування зображення: 1 — крива, що відповідає результатам обчислювального експерименту; 2 — результат ковзного усереднення

Наявні відмінності в обсязі відновленої інформації для СП із близькими значеннями обсягів захищеної інформації зобов'язані існуванню в СП ВВ, збурених у процесі СПр, але незахищених від застосовуваної збурної дії. Із зіставлення всієї сукупності отриманих результатів випливає, що найбільша ефективність декодування, незалежно від конкретики стеганометоду, відповідає найменш чутливим СП, тобто СП із найбільшим обсягом захищеної інформації. Такі результати дають можливість використовувати запропонований метод для вибору контейнера, що забезпечує найбільшу ефективність декодування ДІ при наявній можливості попередньої оцінки очікуваної збурної дії на СП.

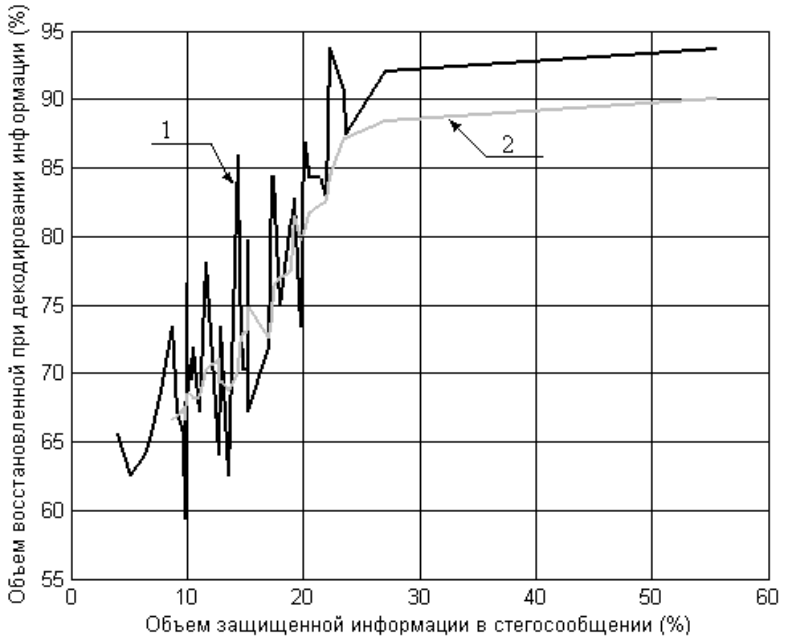


Рис.12.3. Метод відносної заміни величин коефіцієнтів ДКП: 1 — крива, що відповідає результатам обчислювального експерименту; 2 — результат ковзного усереднення

Питання

1. Основні кроки методу порівняльної оцінки чутливості стеганоповідомлень до збурних дій. На основі чого матриця контейнера розглядається в методі як симетрична?
2. Як запропонований метод може бути застосований до множини блоків контейнера?
3. Як визначається обсяг відновленої при декодуванні інформації?

Література

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
2. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.

Змістовий модуль 3. ЗАСТОСУВАННЯ ЗАГАЛЬНОГО ПІДХОДУ ДО ПРОБЛЕМИ ДЕТЕКТУВАННЯ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО СИГНАЛУ

Лекція 13. ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ФОРМАЛЬНИХ ПАРАМЕТРІВ БЛОКІВ ОРИГІНАЛЬНОГО ТА СПОТВОРЕНОГО ЦИФРОВОГО КОНТЕНТУ

План

1. Виявлення порушення цілісності цифрового зображення в результаті накладання шуму
2. Виявлення обробки цифрових контентів засобами графічними редакторами
   2.1. Виявлення розмиття цифрового зображення
   2.2. Формальне представлення корекції яскравості
   2.3. Формальне представлення корекції кольору цифрового зображення

1. Виявлення порушення цілісності цифрового зображення в результаті накладання шуму

Цілісність будь-якого інформаційного контенту є одним з основних критеріїв його захисту, можливості його використання з метою, що відрізняється від розважальної. ЦЗ, які на сьогоднішній день мають значне поширення в різних областях людської діяльності, є такими об'єктами, зміни яких надзвичайно легко здійснити засобами існуючих численних графічних редакторів. І хоча будь-яке порушення цілісності в кожному разі є небажаним, оскільки змінює інформацію оригіналу, залежно від цілей проведених змін їх результат може приводити до різних наслідків: від умовно позитивних (наприклад, при ретушуванні ЦЗ для естетичних цілей) до однозначно негативних (наприклад, коли несанкціоновані зміни проводяться на документах, що мають важливе значення), роблячи задачу виявлення результатів застосування засобів графічних редакторів актуальною.

Однією з самих поширених операцій при порушеннях цілісності ЦЗ є операція накладання шуму, реалізована у всіх графічних редакторах і програмних середовищах, що займаються обробкою зображень. Накладання шуму використовується в ході атаки проти вбудованого повідомлення на стеганоповідомлення (у цьому випадку виявлення шуму дасть можливість організаторам прихованого (стеганографічного) каналу зв'язку виявити факт його моніторингу); накладання шуму на ЦЗ-стеганоповідомлення може використовуватися відправником для маскування наявності вбудованої додаткової інформації (у цьому випадку стеганоалгоритм, що використовується, повинен бути стійким до атак проти вбудованого повідомлення, зокрема, до накладання шуму), для того, щоб завуалювати результати клонування, фотомонтажу і т.д. Тому забезпечення ефективного виявлення результатів накладання різних шумів має велике значення в процесі встановлення оригінальності/порушення цілісності ЦЗ.

Відомо (лекція 3-4), що для оригінальних ЦЗ в більшості $l \times l -$блоків, отриманих шляхом стандартної розбивки матриці зображення, виконується співвідношення:

$$\angle\left(u_1, \overline{\overline{\sigma}}\right) \approx \angle\left(v_1, \overline{\overline{\sigma}}\right) \approx \angle\left(n^O, e_1\right), \qquad (13.1)$$

де $\angle(a,b)$ – кут між відповідними векторами a,b; u_1 і v_1 – відповідно лівий і правий СНВ $l \times l -$блока, що отримані шляхом його нормального сингулярного розкладання, які відповідають максимальному сингулярному числу σ_1 цього блока, $\sigma_1 \geq ... \geq \sigma_l \geq 0$ – СНЧ блока,

$$\overline{\overline{\sigma}} = \left(\sigma_1^2, \sigma_2^2, ..., \sigma_l^{\,2}\right)^T \Big/ \left\| \left(\sigma_1^2, \sigma_2^2, ..., \sigma_l^{\,2}\right)^T \right\| \in R^l, \qquad (13.2)$$

$n^O = \left(1/\sqrt{l}, 1/\sqrt{l}, \ldots, 1/\sqrt{l}\right)^T \in R^l$ – n-оптимальний вектор простору R^l, $e_1 = (1,0,\ldots,0) \in R^l$ – перший вектор стандартного базису R^l. Найбільш прийнятними із практичної точки зору тут є блоки матриці ЦЗ розміром 4×4 пікселя.

Покажемо, що для оригінального ЦЗ кількість $2 \times 2-$ блоків (у відсотковому відношенні до загальної кількості $2 \times 2-$ блоків), для яких кут між векторами u_1 і $\overline{\overline{\sigma}}$ відповідно до (13.1) становить 45^o, приблизно дорівнює кількості $4 \times 4-$ блоків (у відсотковому відношенні до загальної кількості $4 \times 4-$ блоків), для яких кут між векторами u_1 і $\overline{\overline{\sigma}}$ становить 60^o.

Розглянемо блок ЦЗ B_l довільного розміру $l \times l$ з СНЧ $\sigma_1(B_l) \geq \sigma_2(B_l) \geq \ldots \geq \sigma_l(B_l) \geq 0$. Виходячи з (13.1), отримуємо, що

$$\angle\left(u_1, \overline{\overline{\sigma}}\right) = \angle\left(n^O, e_1\right) \qquad (13.3)$$

у випадку, коли $u_1 = n^O$, а $\overline{\overline{\sigma}} = e_1$. Очевидно, що друга рівність означає, що для вектора $\overline{\overline{\sigma}}$, що визначається відповідно до (13.2), має місце співвідношення:

$$\sigma_2(B_l) = \ldots = \sigma_l(B_l) = 0, \qquad (13.4)$$

тобто такий блок B_l визначається єдиною сингулярною трійкою: $(\sigma_1(B_l), u_1(B_l), v_1(B_l))$. Як відомо, така сингулярна трійка відповідає в ЦЗ, головним чином, низькочастотній складовій (тобто областям ЦЗ з малими перепадами значень яскравості – фоновим областям). Таким чином, блоки ЦЗ, для яких (13.3) виконується точно, належать, головним чином, областям зображення з малими перепадами значень яскравості. Однак умова малого перепаду яскравості в загальному випадку не гарантує в точності умову (13.4). Більш того, на практиці перевірено, що для блоків оригінального ЦЗ, для яких $l \geq 8$, умова (13.4) не буде виконуватися в точності практично ніколи навіть в областях з малими перепадами значень яскравості, оскільки малі перепади значень у загальному випадку не гарантують лінійну залежність стовпців (рядків), що містять достатньо велику кількість ($l \geq 8$) елементів, матриці (блоку матриці). Наприклад, для блоку B_8 (рис.13.1(б)) сингулярний спектр має вигляд:

$$1223.3,\ 3.1,\ 2.1,\ 1.6,\ 1.2,\ 1.0,\ 0.3,\ 0.1, \qquad (13.5)$$

хоча сам блок очевидно належить фоновій частині ЦЗ (рис.13.1(а)). Однак з урахуванням кореляції значень яскравості пікселів, що знаходяться поряд, яка має місце в оригінальних ЦЗ, для блоків малого (і це принципово важливо) розміру ($l \leq 4$) в області з малими перепадами яскравості співвідношення (13.4) буде мати місце, причому, оскільки найближчі сусіди пікселя – це пікселі, що знаходяться від нього ліворуч, праворуч, зверху, знизу, то міра лінійної залежності стовпців (рядків) блоку 4×4 буде порівнянна з аналогічним показником для $2 \times 2-$ блоків, отриманих стандартною розбивкою блоку 4×4. Так для приклада, представленого на рис.13.1, сингулярний спектр верхнього лівого 4×4-блоку B_8 (рис.13.1(б)) визначається як

$$609.5,\ 0.9,\ 0.0,\ 0.0, \qquad (13.6)$$

а для $2\times 2-$ блоків, що його складають, сингулярні спектри будуть визначатися наступним чином:

$$305.5,\ 0.4;\quad 305.0,\ 0;\quad 304.5,\ 0.4;\quad 304,\ 0. \qquad (13.7)$$

Якщо порівняти отримані результати (13.6) і (13.7) для B_4 і блоків B_2, що його складають, то треба відзначити, що відповідності між ними не випадкові. Дійсно, можна показати, що для ЦЗ з $n\times n-$матрицею F, елементи якої $f_{ij}, i,j=\overline{1,n}$, а СНЧ – $\sigma_i(F), i=\overline{1,n}$, має місце співвідношення:

$$\sum_{i,j=1}^{n} f_{ij}^{2} = \sum_{i=1}^{n} \sigma_i^2(F). \qquad (13.8)$$

У силу значної корельованості у фоновій області значень яскравості пікселів у межах B_4 з (13.8) буде випливати, що для такого блоку

$$\sigma_1^{\,2}(B_4) = \sum_{i,j=1}^{4} \left(b_{ij}^{(4)}\right)^2, \qquad (13.9)$$

де $b_{ij}^{(4)}$, $i,j=\overline{1,4}$, – елементи матриці B_4, що порівнянні між собою. Тоді (13.9) можна представити в вигляді:

$$\sigma_1^{\,2}(B_4) \approx 4\left(b_{11}^{(4)}\right)^2 + 4\left(b_{13}^{(4)}\right)^2 + 4\left(b_{31}^{(4)}\right)^2 + 4\left(b_{33}^{(4)}\right)^2 \approx \sigma_1^{\,2}\left(B_2^{(1)}\right) + \sigma_1^{\,2}\left(B_2^{(2)}\right) + \sigma_1^{\,2}\left(B_2^{(3)}\right) + \sigma_1^{\,2}\left(B_2^{(4)}\right) \approx$$

$$\approx 4\sigma_1^{\,2}\left(B_2^{(1)}\right) \approx 4\sigma_1^{\,2}\left(B_2^{(2)}\right) \approx 4\sigma_1^{\,2}\left(B_2^{(3)}\right) \approx 4\sigma_1^{\,2}\left(B_2^{(4)}\right),$$

де $B_2^{(i)}, i=\overline{1,4}$ – $2\times 2-$блоки, які є результатом стандартної розбивки B_4, звідки

$$2\sigma_1\left(B_2^{(1)}\right) \approx 2\sigma_1\left(B_2^{(2)}\right) \approx 2\sigma_1\left(B_2^{(3)}\right) \approx 2\sigma_1\left(B_2^{(4)}\right) \approx \sigma_1(B_4),$$

що й ілюструє приклад, наведений на рис.13.1(б). Подібна ситуація очевидно буде мати місце для СНЧ блоків B_{2^k} і $B_{2^{k-1}}$ (на які блок B_{2^k} розбивається стандартним чином) у випадку, коли B_{2^k} належить області ЦЗ із малими перепадами значень яскравості (див. сингулярні спектри (13.5) і (13.6) для B_8 і B_4 відовідно).

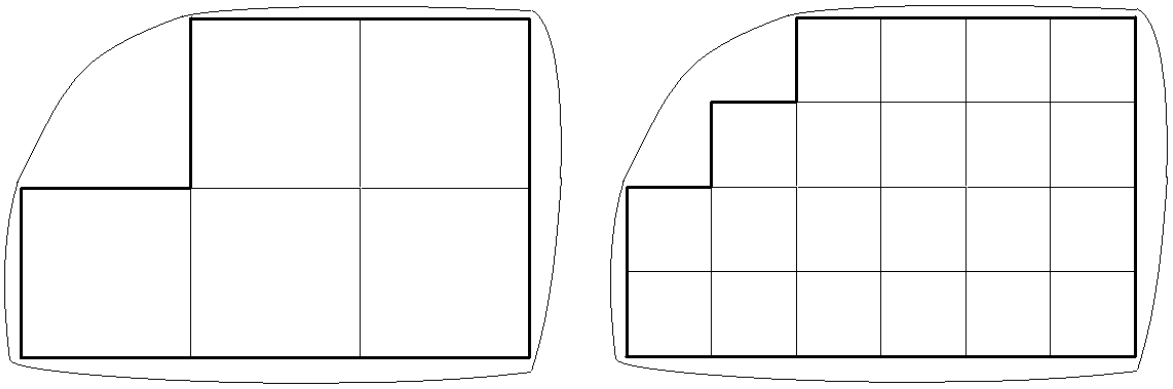
$B_8 =$

152	152	152	152	153	154	153	153
153	154	153	153	154	154	154	153
152	153	152	152	153	154	154	152
152	152	152	152	152	152	154	153
153	153	153	153	153	152	153	154
153	153	153	153	153	152	153	153
154	153	153	153	153	153	153	153
153	152	152	154	154	153	153	153

а б

Рис.13.1. Приклад відповідності, що має місце між блоками різного розміру області оригінального ЦЗ із малими перепадами значень яскравості: а – вхідне ЦЗ із покажчиком на розглянутий блок; б – матриця $8\times8-$блоку ЦЗ з вказаної області

Таким чином, для $4\times4-$ і $2\times2-$блоків областей ЦЗ із малими перепадами значень яскравості співвідношення (13.3) буде виконуватися з дуже незначною похибкою за рахунок того, що співвідношення (13.4) буде виконуватися практично точно. Області ЦЗ із малими перепадами значень яскравості, що складаються з $4\times4-$, $2\times2-$блоків, у силу малих розмірів блоків, що розглядаються, будуть відрізнятися по площі дуже незначно (рис.13.2), а це означає, що відносні (стосовно загального числа блоків зображення) кількості $4\times4-$, $2\times2-$блоків у зазначених областях будуть порівнянні одна з іншою. Таким чином, кількості $4\times4-$ і $2\times2-$блоків в ЦЗ, для яких $\angle\left(u_1,\overline{\overline{\sigma}}\right)\approx\angle\left(n^O,e_1\right)$, будуть в оригінальному ЦЗ відрізнятися дуже незначно. Кількісно відмінності будуть залежати від формату ЦЗ. Можна стверджувати, що для оригінальних ЦЗ у форматі з втратами ця відмінність буде менше по абсолютній величині, ніж для ЦЗ у форматі без втрат. Це пов'язано з тим, що при збереженні ЦЗ із втратами, результатом чого є зменшення внеску високочастотної (і, можливо, середньочастотної) складової, найменші СНЧ блоків зменшуються в порівнянні з їхніми значеннями для цього ж ЦЗ, але збереженого спочатку у форматі без втрат. Найменші СНЧ блоків зображення із втратами можуть стати порівнянними з нулем навіть у тих блоках, які не відповідають областям з незначними перепадами яскравості.



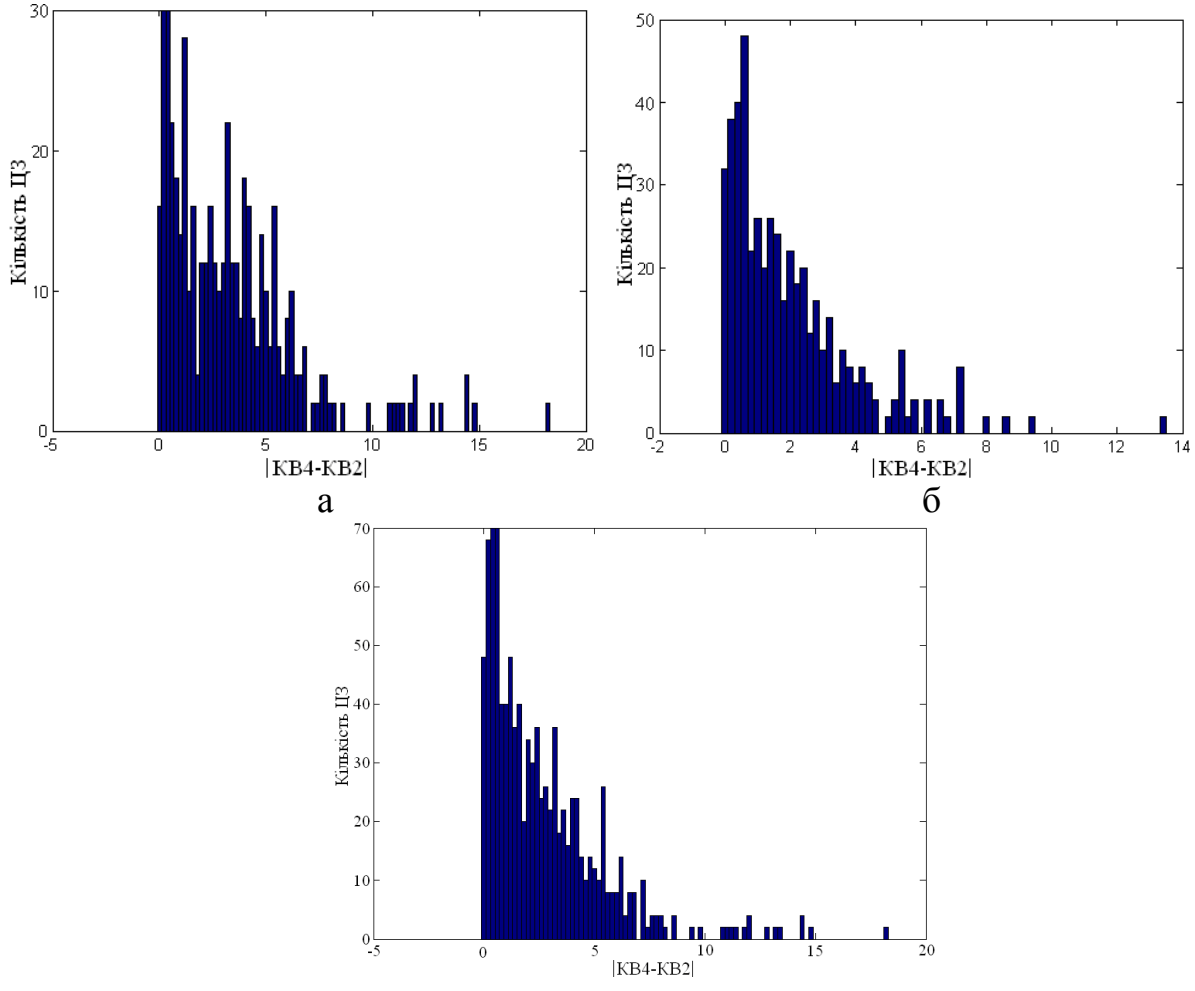
а б

Рис.13.2. Область ЦЗ із малими перепадами значень яскравості й блоки розбивки матриці зображення малих розмірів, що її складають: а – $4\times4-$блоки; б – $2\times2-$блоки

Для практичного підтвердження отриманого висновку був проведений обчислювальний експеримент, у якому були задіяні ЦЗ з різних баз:

- множина M_1: 200 ЦЗ розміром 1000×1000 пікселів в форматі Tif;
- множина M_2: 300 ЦЗ розміром 500×500 пікселів в форматі Tif;
- множина M_3: 500 ЦЗ розміром 1000×1000 пікселів в форматі Jpeg.

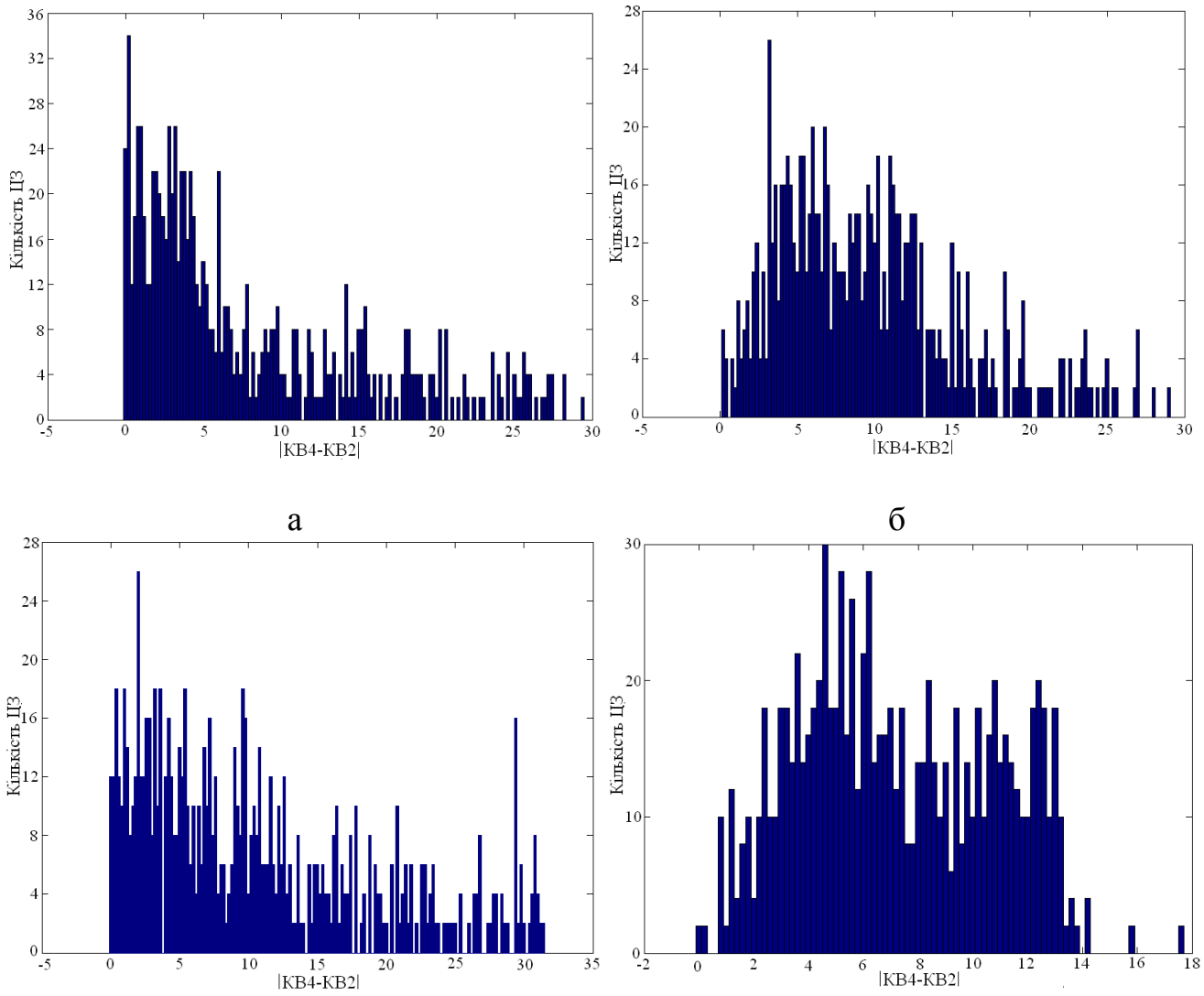
У ході експерименту матриця кожного ЦЗ розбивалася стандартним чином на блоки розміром 2×2, для кожного блоку визначався кут між векторами u_1 і $\overline{\overline{\sigma}}$, після чого будувалася гістограма значень таких кутів, для якої знаходилася мода m_2 і значення $KB2$ гістограми в моді. Потім ЦЗ розбивалося на блоки 4×4 пікселя, після чого виконувалися аналогічні дії й визначалося значення $KB4$ – кількість блоків розміром 4×4 в ЦЗ (у відсотковому відношенні до загального числа блоків), для яких кут між u_1 і $\overline{\overline{\sigma}}$ дорівнює значенню моди m_4 відповідної гістограми. У ході експерименту для ЦЗ із $M_1\cup M_2$ мода гістограми $m_2\neq45^o$ для 1 ЦЗ, $m_4\neq60^o$ для 4 ЦЗ (що складає 0.2% і 0.8% від загальної кількості розглянутих ЦЗ без втрат відповідно), для всіх інших ЦЗ, зокрема зображень із множини M_3, $m_2=45^o$, $m_4=60^o$, що відповідає (13.3). Для кожного ЦЗ знаходилося значення $KB4-KB2$. Для отриманої множини значень $|KB4-KB2|$ по всім ЦЗ будувалася гістограма (рис.13.3). При цьому середнє значення для $|KB4-KB2|$ по множині $M_1\cup M_2$ склало 3.5%, по множині M_3 – 2.1%, по $M_1\cup M_2\cup M_3$ – 2.8%, що повністю відповідає отриманим вище теоретичним висновкам про незначну відмінність $KB1$ і $KB2$ для оригінальних ЦЗ.



в

Рис.13.3. Гістограми значень $|KB4-KB2|$ для оригінальних ЦЗ: а – для ЦЗ в форматі без втрат (множина $M_1 \bigcup M_2$); б – для ЦЗ в форматі з втратами (множина M_3); в – для ЦЗ з $M_1 \bigcup M_2 \bigcup M_3$

Накладання шуму на оригінальне ЦЗ, змінюючи значення яскравості пікселів, змінює (частіше – зменшує) кореляцію між сусідніми пікселями, змінює в загальному випадку не тільки кількісно, але і якісно характеристики різних областей ЦЗ: на фонових областях оригінального зображення при накладанні шуму можуть виникнути перепади яскравості, більш значні, ніж у вхідному зображенні. Все це приводить до того, що $2\times2-$ і $4\times4-$блоки навіть у межах фонової області ЦЗ будуть поводитися вже не настільки однаково, як в оригінальному зображенні. Поведінка молодших СНЧ (порівнянність із нулем) може бути порушена як для $4\times4-$, так і для $2\times2-$блоків. Очікуваним тут буде можливе порушення положення моди гістограми значень кутів між векторами u_1 і $\overline{\overline{\sigma}}$ блоків відносно оригінального ЦЗ (це порушення однозначно буде трактуватися як показник порушення цілісності ЦЗ), а також більша відмінність в значеннях $KB2$ і $KB4$, що підтверджується результатами обчислювального експерименту, наведеними для $M_1 \bigcup M_2 \bigcup M_3$ на рис.13.4, в табл.13.1.



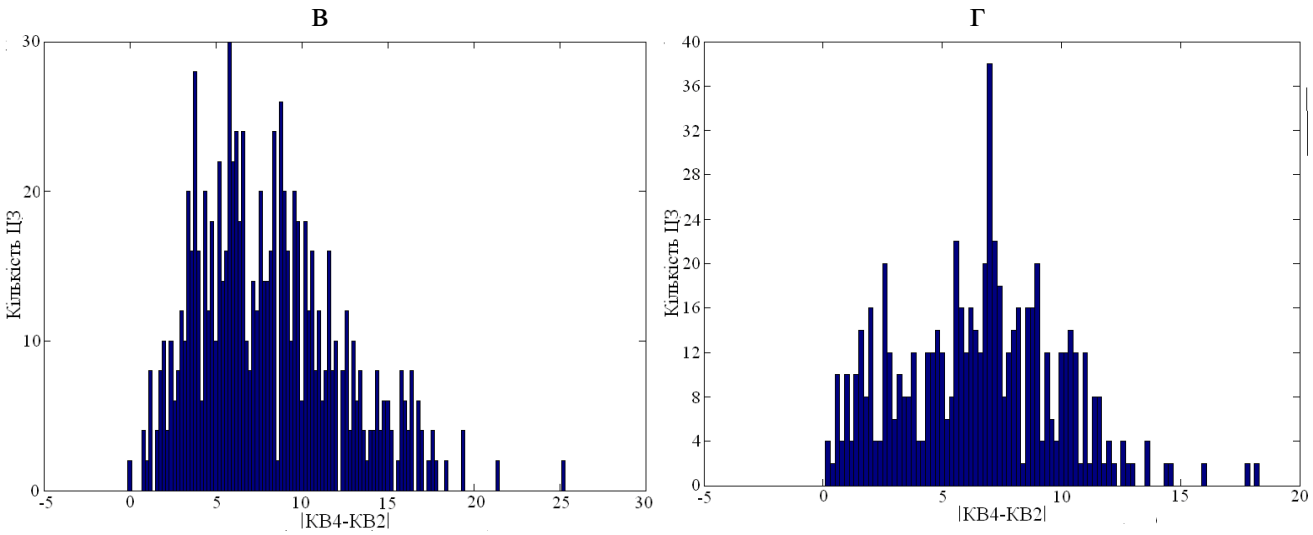


Рис.13.4. Гістограми значень $|KB4-KB2|$ в умовах накладання на ЦЗ: а – гауссівського шуму з нульовим математичним очікуванням і D=0.0001; б – гауссівського шуму з нульовим математичним очікуванням і D=0.001; в – мультиплікативного шуму з D=0.001; г – мультиплікативного шуму з D=0.01; д – пуассонівського шуму; е – шуму «сіль-перець» з D=0.01

Таблиця 13.1 – Середні значення $|KB4-KB2|$ при накладанні шумів на ЦЗ з $M_1 \cup M_2 \cup M_3$ (%)

Гауссівський шум з нульовим математичним очікуванням		Мультиплікативний шум		Пуассонівський шум	Шум «сіль-перець» з D=0.01
D=0.0001	D=0.001	D=0.001	D=0.01		
7.9	9.7	10.7	7.2	8.1	6.5

Параметри шумів, що накладалися, вибиралися таким чином, щоб уникнути (значних) візуальних споворень зображень, які кількісно оцінювалися за допомогою різницевого показника PSNR – «пікового відношення сигнал-шум» (табл.13.2).

Таблиця 13.2 – Середні значення $PSNR$ при накладанні шумів на ЦЗ з $M_1 \cup M_2 \cup M_3$ (dB)

Гауссівський шум з нульовим математичним очікуванням		Мультиплікативний шум		Пуассонівський шум	Шум «сіль-перець» з D=0.01
D=0.0001	D=0.001	D=0.001	D=0.01		
40	32	36	29	31	26

Як видно з отриманих результатів, середні по експерименту значення $|KB4-KB2|$ значно відрізняються для оригінальних ЦЗ і ЦЗ, що зазнали накладання шуму, як і якісний вид гістограм значень $|KB4-KB2|$: для оригінальних ЦЗ мода гістограм близька до нуля й для множини $M_1 \cup M_2$, і для M_3, і для $M_1 \cup M_2 \cup M_3$, причому кількість ЦЗ, для яких

$|KB4 - KB2|$ далеко від нуля, очевидно значно менше тих, для яких $|KB4 - KB2|$ близько до нуля (рис.13.3), чого не можна сказати про ЦЗ, що зазнали накладання шуму (рис.13.4).

2.Виявлення обробки цифрових контентів засобами графічними редакторами

2.1. Виявлення розмиття цифрового зображення

Як показує практика й факти, відомі з відкритих джерел, одним з обов'язкових використовуваних програмних інструментів обробки ЦЗ при його несанкціонованій зміні є розмиття (РЗ) (хоча РЗ часто використовується у фотоіндустрії для зовсім «некримінальних» цілей: додання певного ефекту як зображенню в цілому, так і його частині, наприклад, для акцентування уваги на деякому об'єкті (об'єкт - чіткий, у фокусі, а інша область розмита); усунення дефектів зображення, виникаючих, наприклад, при скануванні, при компресії; для усунення на зображенні природніх дефектів шкіри як звичайних (родимки, подряпини й т.д.), так і вікових (зморшки)).

Відповідно до розробленої загальної методології аналізу властивостей, стану й технології функціонування довільної інформаційної системи цей аналіз зводиться до аналізу визначальних ІС математичних параметрів - СНЧ і СНВ матриці (матриць), що відповідає системі. Відмінними рисами СНЧ матриці (блоків матриці) розмитого ЦЗ є те, що швидкість росту найменших СНЧ спектра відповідної матриці (при використанні для них кусочно-лінійної інтерполяції) якісно відрізняється від відповідної характеристики вхідного зображення - вона значно менше (типовий приклад наведений на рис.13.5). Отриманий ефект пояснюється наступним чином. РЗ приводить до зменшення високочастотної складової сигналу (візуальним результатом даного інструмента обробки є згладжування контурів), а, враховуючи відповідність між частотними складовими й сингулярними трійками матриці сигналу, СНЧ при застосуванні РЗ зменшуються певним чином: найбільше «постраждають» найменші (ті, що відповідають високочастотній складовій ЦЗ) і, можливо, середні по величині СНЧ: швидкість їх росту буде близька до нуля (причому, відмінність від нуля тим менше, чим більше радіус РЗ (рис.13.5 – див. СНЧ 6-12).

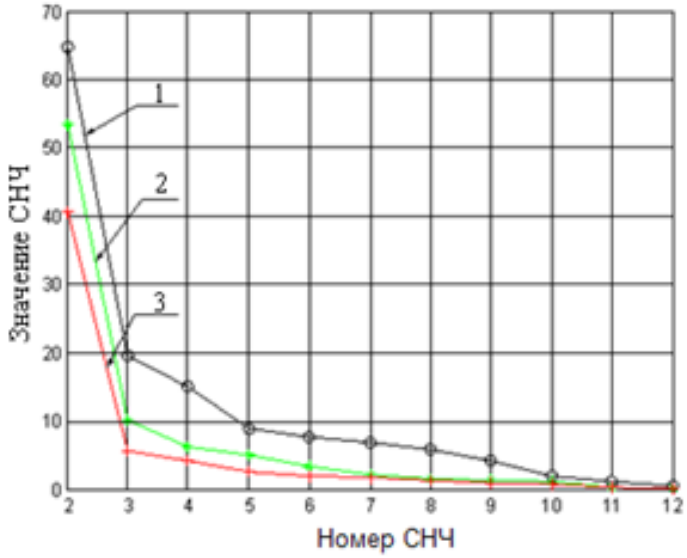


Рис.13.5. Інтерполяційний сплайн першого ступеня для множини СНЧ тестового ЦЗ: 1 – подане ЦЗ; 2 – розмите з радіусом 1; 3 – розмите з радіусом 2

Очевидно, що використовувати для сукупної характеристики досліджуваних СНЧ - оцінки їх швидкості росту - інтерполяційний сплайн (будь-якого ступеня) при автоматизації процесу незручно: ця швидкість у загальному випадку повинна була б обчислюватися на

кожному відрізку із двох сусідніх СНЧ, змінювалася б від одного СНЧ до іншого. У цьому випадку нам необхідно було б визначити границі для швидкості росту в розмитому ЦЗ (РЦЗ) і нерозмитому ЦЗ (НРЦЗ), що значно ускладнило б процес.

Будемо використовувати для представлення сукупності розглянутих малих і середніх СНЧ замість інтерполяційної функції апроксимуючу. Це значно спростить процес обчислення наближеного значення швидкості росту досліджуваних СНЧ. У якості апроксимуючої функції будемо використовувати многочлен ступеня k. Для спрощення процесу побудови функції, що наближає, має сенс взяти $k=1$.

Для одержання числових параметрів і їх граничних значень, які дозволять відокремити РЦЗ від НРЦЗ, необхідно кількісно оцінити швидкість росту найменших СНЧ спектра відповідних матриць, використовуючи для цього апроксимуючий многочлен першого ступеня. Із цією метою в середовищі Matlab був проведений обчислювальний експеримент, у якому використовувалося більше 1000 різних ЦЗ у форматі jpeg (з різним параметром «якість»). У ході експерименту зображення піддавалися операції РЗ в Photoshop за допомогою фільтра «Розмиття по Гауссу». Вибір даного фільтра обумовлений частотою його використання з різними цілями, у тому числі, і для приховування слідів фальсифікації ЦЗ. Основним параметром фільтра, що обирається, є радіус розмиття, який скрізь нижче навмисно брався мінімальним (1 піксель) – ситуація, яка найбільш складно «виловлюється»; збільшення радіуса розмиття збільшує якісні й використовувані нижче кількісні відмінності РЦЗ й НРЦЗ.

Доказ оригінальності ЦЗ є важливим завданням у багатьох областях людської діяльності. Конкретизуємо область, що цікавить нас, судовими розглядами. У силу специфіки задачі якість зображення, що надається, наприклад, як речовинний доказ, повинна бути прийнятною. Це означає, що на зображені неприпустима наявність артефактів, які можуть виникнути після стиску. Крім того, погана якість зображення сама по собі викликає сумнів у оригінальності, що не дозволить розглядати його як речовинний доказ. При збереженні зображення в jpeg в Photoshop, який може використовуватися в стандартному, оптимізованому й прогресивному виді, можливі 65 варіантів такого збереження залежно від значення параметра «якість», який далі позначається Q (Q приймає значення 0,1,2,...,12). Шляхом суб'єктивного ранжирування було встановлено, що при $Q \in \{0,1,...,7\}$ артефакти на ЦЗ в більшому або меншому ступені помітні, крім того, як показує практика, гарне візуальне сприйняття досягається вже при $Q=9, Q=10$. Тому дослідження проводилися для $Q \in \{8,9,10\}$.

Найбільш явно швидкість росту малих і середніх СНЧ матриці (матриць) РЦЗ буде відрізнятися від аналогічної характеристики для НРЦЗ тоді, коли вхідне зображення було в найкращій якості ($Q=10$).Дійсно, у цьому випадку контури НРЦЗ будуть найбільш чіткими, високочастотна складова сигналу буде найбільш значною, а найменші СНЧ відповідної матриці будуть найбільшими, маючи найбільшу швидкість росту в порівнянні з $Q=8, Q=9$. У силу цього після РЗ ефект зменшення найменших СНЧ і їх швидкості росту буде найбільш помітний (як буде відзначено нижче, розроблений метод у цьому випадку практично не дає помилок). Найбільші «складності» для пропонованого методу виникнуть при $Q=8$, оскільки при такій якості високочастотна складова сигналу, найменші СНЧ відповідної матриці (матриць) і швидкість їх росту самі по собі досить малі ще до обробки зображення засобом РЗ.

Нехай F — $n \times m$-матриця ЦЗ. Розіб'ємо цю матрицю стандартним чином на блоки 8×8, загальна кількість B яких:

$$B = \left[\frac{n}{8}\right] \cdot \left[\frac{m}{8}\right] = \underline{O}(mn) \qquad (13.10)$$

де $[\bullet]$ - ціла частина аргументу, для кожного з яких обчислимо множину СНЧ. Для п'яти найменших СНЧ кожного блоку побудуємо лінійну апроксимуючу функцію, кутовий коефіцієнт якої є наближеним значенням швидкості росту досліджуваних СНЧ. ЦЗ, що піддається експертизі, поставимо у відповідність матрицю розміру $\left[\frac{n}{8}\right] \times \left[\frac{m}{8}\right]$, кожний елемент якої відповідає блоку з тими ж індексами й дорівнює швидкості росту найменших п'яти СНЧ блоку - матрицю швидкості росту (МШР). МШР для НРЦЗ і РЦЗ якісно відрізняються друг від друга.

Щоб автоматизувати процес розпізнавання й більш точно визначити поріг значень МШР для зображення до й після РЗ, введемо вектор середніх значень (ВСЗ), який є результатом усереднення значень МШР по стовпцях (нічого принципово не зміниться, якщо при побудові ВСЗ брати усереднення по рядках МШР). Для ЦЗ «Маша» (рис.13.6) графічні представлення ВСЗ і апроксимуючі їхні лінійні функції, наведені для більшої наочності, дані на рис.13.7.

Рис.13.6. Тестове ЦЗ «Маша»

Для найбільш цілісного аналізу ВСЗ уведемо два параметри: максимальне ($VMV_{\max}$) і середнє (VMV_c) значення ВСЗ. Це дає можливість відстежити, у якому діапазоні значень перебуває основна частина елементів МШР до й після РЗ. У ході численних експериментів було виявлено, що порогом для цих параметрів, що відокремлюють переважну більшість РЦЗ від НРЦЗ, є 1. Так, якщо $VMV_{\max}$ і VMV_c більше 1, то зображення не розмите, якщо менше 1, то зображення розмите або не містить контурів (така ситуація можлива для фонових зображень (або фонових частин ЦЗ). Однак, у силу специфіки розглянутого завдання надзвичайно мала ймовірність виникнення необхідності аналізу відеоматеріалу, що представляє із себе просто фонове зображення). На практиці можливий варіант, коли VMV_c менше 1, а $VMV_{\max}$ більше 1. Така ситуація можлива у випадку, коли зображення зроблене в режимі «макрозйомка», а також у тому випадку, коли $Q = 8$ (і менше). Цей варіант передбачений розробленим алгоритмом, що сигналізує про РЗ (рис.13.8). У цьому випадку потрібні додаткові дослідження.

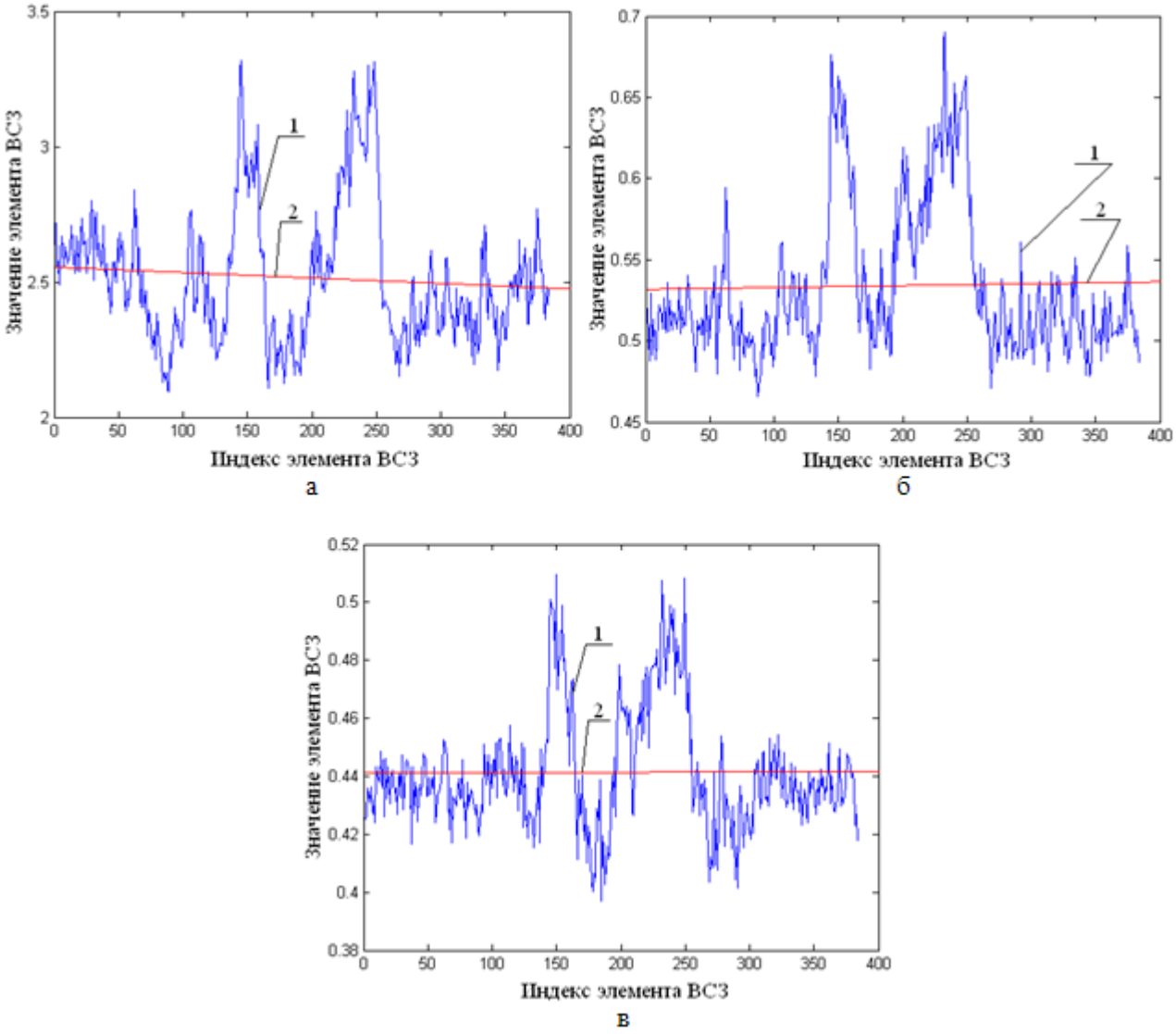


Рис.13.7. 1 - Графічне представлення ВСЗ для тестового ЦЗ «Маша», 2 – лінійна апроксимація ВСЗ: а – до розмиття; б – після розмиття (радіус – 1 піксель); в – після повторного розмиття (радіус – 1 піксель)

Для більшої наочності відмінностей в отриманих результатах матриці МШР ставиться у відповідність сукупність графіків (далі - результуючу сукупність (РС)), кожний з яких відповідає стовпцю МШР і відображає залежність між номером елемента в стовпці і його значенням. РС для тестового ЦЗ «Маша», яка дає типову якісну картину, представлена на рис.13.9, де кожний графік РС має индивідуальний колір. Як видно, діапазон значень (ДЗ) найбільшої «щільності» РС для НРЦЗ набагато ширше аналогічної характеристики для РЦЗ, а повторне розмиття практично не змінює якісну картину в порівнянні з первинним розмиттям (порівн. рис.13.9(б) і 13.9(в)). Аналогічна картина спостерігається й для ВСЗ (порівн. рис.13.7(б) і 13.7(в)). Дана особливість дає можливість для уточнення висновку про розмиття ЦЗ.

Шаг 1. Разбить тестируемое изображение стандартным образом на B 8×8-блоков.

Шаг 2. Для каждого полученного блока b_{ij} (i, j - номера блоковой строки и столбца соответственно для рассматриваемого блока; $1 \le i \le \left[\frac{n}{8}\right]$, $1 \le j \le \left[\frac{m}{8}\right]$):

2.1. Вычислить множество СНЧ;

2.2. Для пяти наименьших СНЧ построить линейную аппроксимирующую функцию, угловой коэффициент которой a_{ij} является приближенным значением скорости роста исследуемых СНЧ.

Шаг 3. По результатам, полученным на шаге 2, построить матрицу S скорости роста, элементы которой

$$s_{ij} = a_{ij}\ ,\ 1 \le i \le \left[\frac{n}{8}\right],\ 1 \le j \le \left[\frac{m}{8}\right].$$

Шаг 4. Построить ВСЗ VMV, элементы которого v_j, $1 \le j \le \left[\frac{m}{8}\right]$. Для этого

4.1. Для каждого j-го столбца МСР S ($1 \le j \le \left[\frac{m}{8}\right]$) найти среднее арифметическое значение s_j^C;

4.2. $v_j = s_j^C$.

Шаг 5. Вычислить максимальное $VMV_{\max}$ и среднее VMV_c значения ВСЗ.

Шаг 6 (***проверка***).

6.1. Если ($VMV_{\max} < 1 \wedge VMV_c < 1$), то *тестируемое ЦИ подвергалось операции РИ* или не содержит контуров;

6.2. Если ($VMV_{\max} > 1 \wedge VMV_c > 1$), то *тестируемое ЦИ не подвергалось РИ*;

6.3. Иначе ЦИ *возможно* размыто или снято в режиме «макросъемка». Для окончательного ответа необходимы дополнительные исследования.

Рис.13.8. Алгоритм відокремлення РЦЗ від НРЦЗ

Додаткові дослідження

Розглянемо докладно пункт 6.3 алгоритму відокремлення РЦЗ від НРЦЗ. Однією з можливих причин виникнення ситуації 6.3 є одержання вхідного НЦЗ в режимі «макрозйомка», коли зображення являє собою візуально чіткий об'єкт (об'єкти) на візуально розмитому (ненавмисно) малоінформаційному фоні. Залежно від об'єктива й інших параметрів фотокамери, якою було зроблено ЦЗ, а також від відстані до об'єкта, ступінь розмиття фона при макрозйомці може бути різною. Не завжди можна точно визначити, розмито зображення, або воно знято в режимі «макрозйомка». Якщо $VMV_c < 1$, але є значення ВСЗ, більше 1, вони можуть відповідати тій частині ЦЗ, у якій розташований чіткий об'єкт. У цьому випадку необхіднозвернутися до додаткової перевірки:

Крок 1. Навмисно розмити зображення, що тестується, використовуючи фільтр «Розмиття по Гауссу», вибравши при цьому найменший радіус - 1 піксель;

Крок 2. Побудувати для отриманого після кроку 1 ЦЗ РС і ВСЗ.

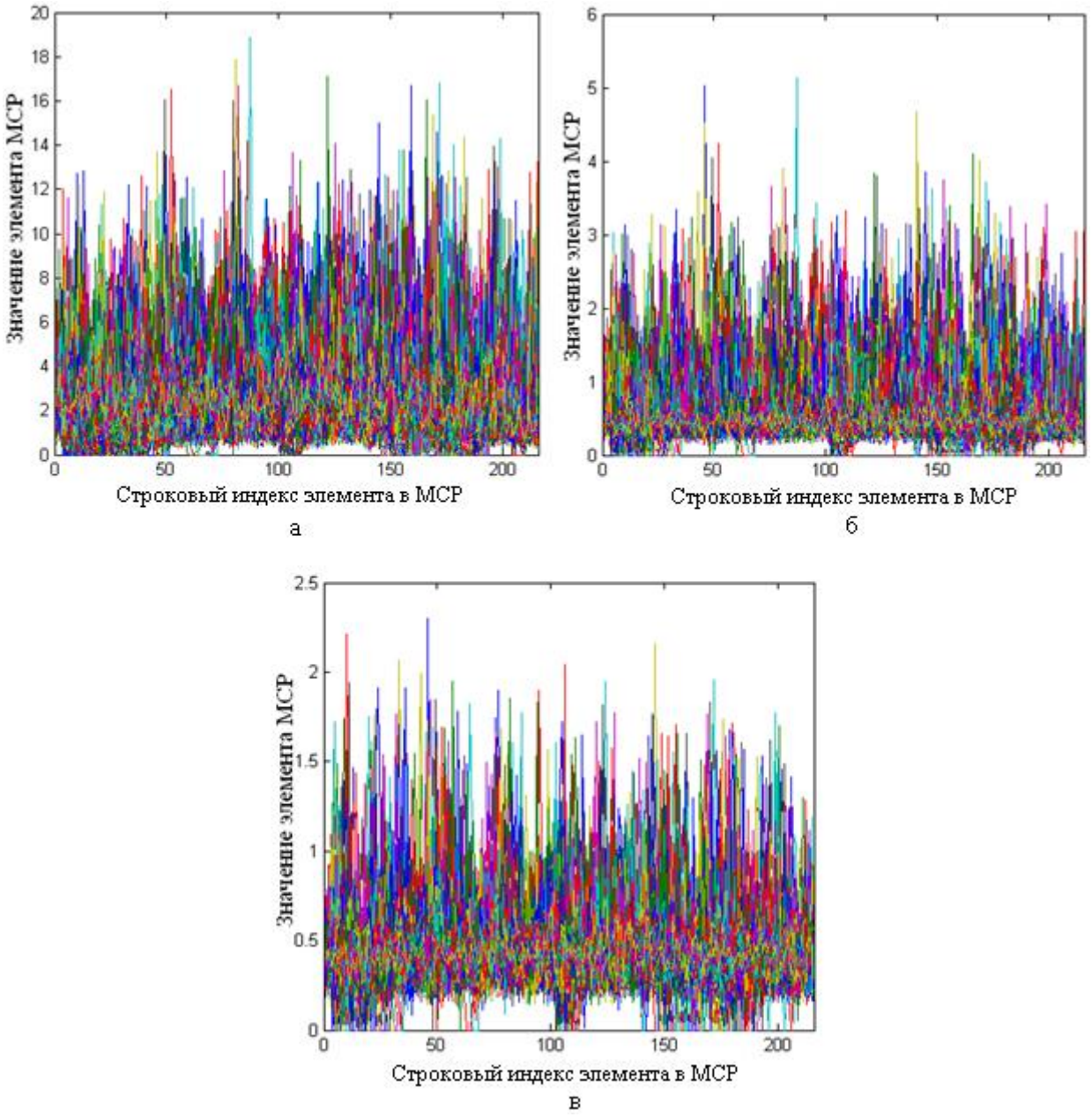


Рис.13.9. РС для ЦЗ «Маша»: а – до розмиття; б – після розмиття (радіус – 1 піксель); в – після повторного розмиття (радіус – 1 піксель)

Крок 3 (аналіз). Порівняти РС і ВСЗ до й після проведеного РЗ. Якщо зображення вже було розмито з радіусом, більшим або рівним 1, то зроблене розмиття з радіусом 1 піксель, будучи для нього повторним, принципово не змінить ні основну частину РС, згладивши тільки деякі найбільші значення, ні ВСЗ (див. рис.13.7(б,в), 13.9(б,в)). Якщо ж тестоване ЦЗ не було розмито спочатку, то зроблене навмисно РЗ буде для нього першим, і внесе значні зміни у високочастотну складову сигналу зображення, а тому в СНЧ відповідних матриць і, як наслідок, у РС, ВСЗ (див. рис.13.7(а,б), 13.9(а,б)). При автоматизації процесу додаткової перевірки розмиття вважається первинним, якщо після виконання операції РЗ ДЗ РС і $VMV_{\max}$ зменшуються в ≈3 і більше, ≈2 і більше разів відповідно.

Для ЦЗ, знятого в режимі «макрозйомка» й не зазнавшего навмисне РИ, наведеного на рис.13.10, має місце висновок 6.3. При цьому РС і ВСЗ мали вигляд, представлений на рис.13.11(а), 13.12(а). Розмиємо «підозріле» ЦЗ з радіусом 1 (РС і ВСЗ мають вигляд, представлений на рис.13.11(б), 13.12(б) відповідно). Як видно з порівняння рис.13.11(а) і

13.11(б), $VMV_{\max}$ після розмиття зменшався більш, ніж в 3 рази; порівняння рис.13.12(а) і 13.12(б) показує зменшення ДЗ РС в ≈3 рази, що дозволяє зробити висновок про те, що зображення не було розмито спочатку.

Рис.13.10. ЦЗ, зняте в режимі «макрозйомка»

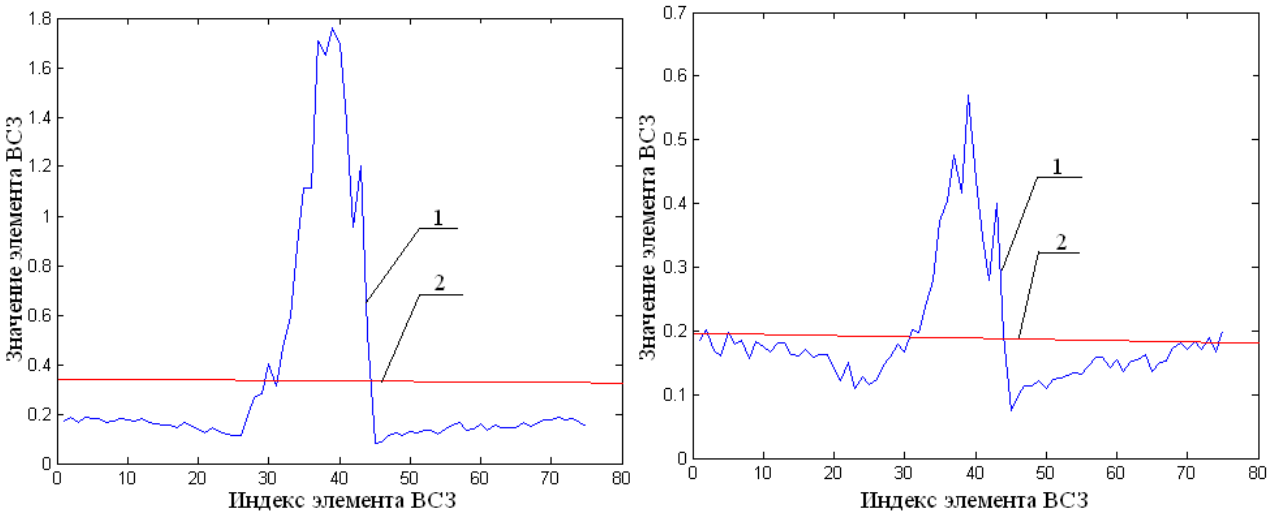


Рис.13.11. 1 - Графічні представлення ВСЗ для тестового ЦЗ, знятого в режимі «макрозйомка», 2 - лінійна апроксимація ВСЗ: а - до розмиття; б - після розмиття (радіус - 1 піксель)

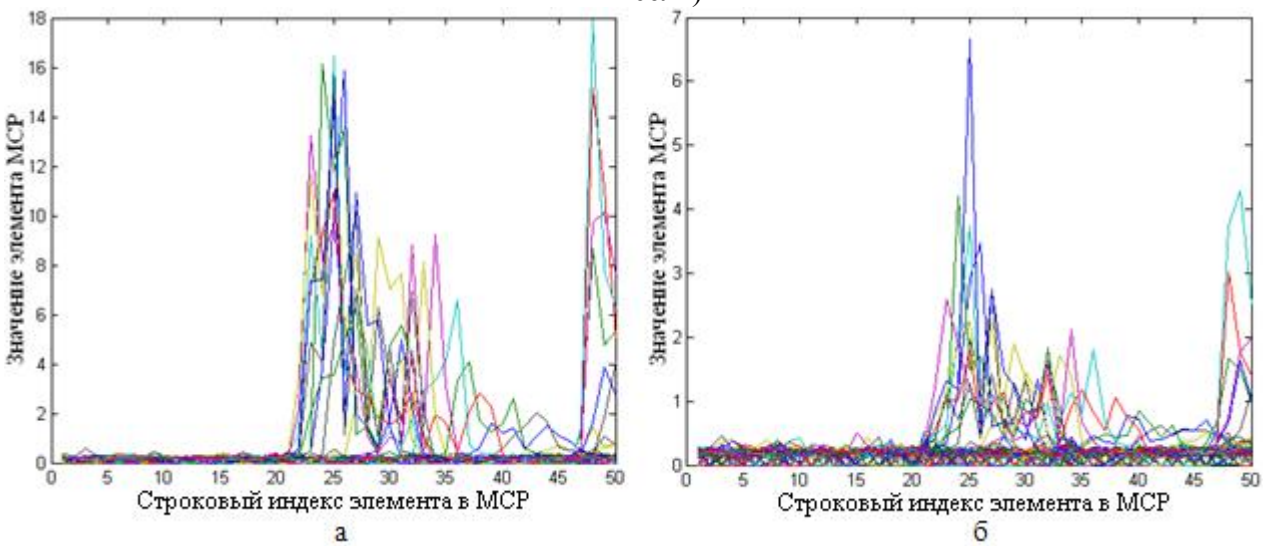


Рис.13.12. РС для ЦЗ, знятого в режимі «макрозйомка»: а – до розмиття; б – після розмиття (радіус – 1 піксель)

Якщо тестуємо зображення не мало спочатку високу якість, то також рекомендується проводити додаткову перевірку, як при виникненні ситуації 6.3, щоб збільшити ймовірність правильного результату роботи запропонованого алгоритму. Для ілюстрації розглянемо приклад ЦЗ, наведеного на рис.13.13.

Рис.13.13. ЦЗ в форматі Jpeg (Q=8)

Це зображення не зазнало РЗ, хоча при роботі запропонованого алгоритму із цим ЦЗ, як видно з рис.13.14(а) ($VMV_{\max} < 1$ і $VMV_c < 1$), видається результат: «Фото розмите або не містить контуров».

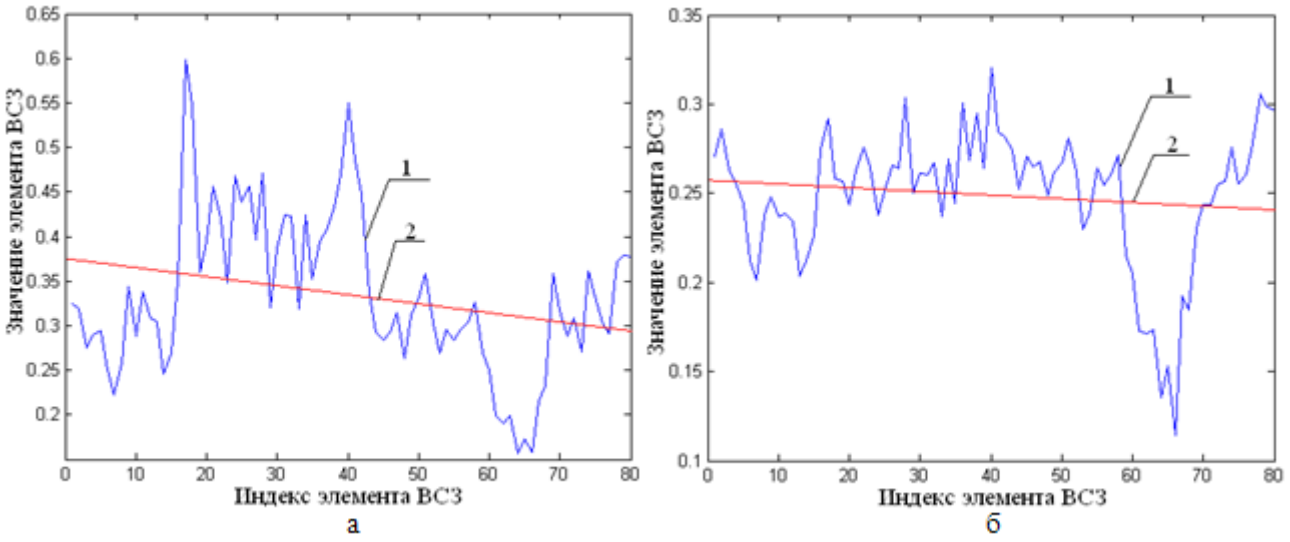


Рис.13.14. 1 - Графічне представлення ВСЗ для тестового ЦЗ в форматі jpeg з $Q = 8$, 2 – лінійна апроксимація ВСЗ: а – до розмиття; б – після розмиття (радіус – 1 піксель)

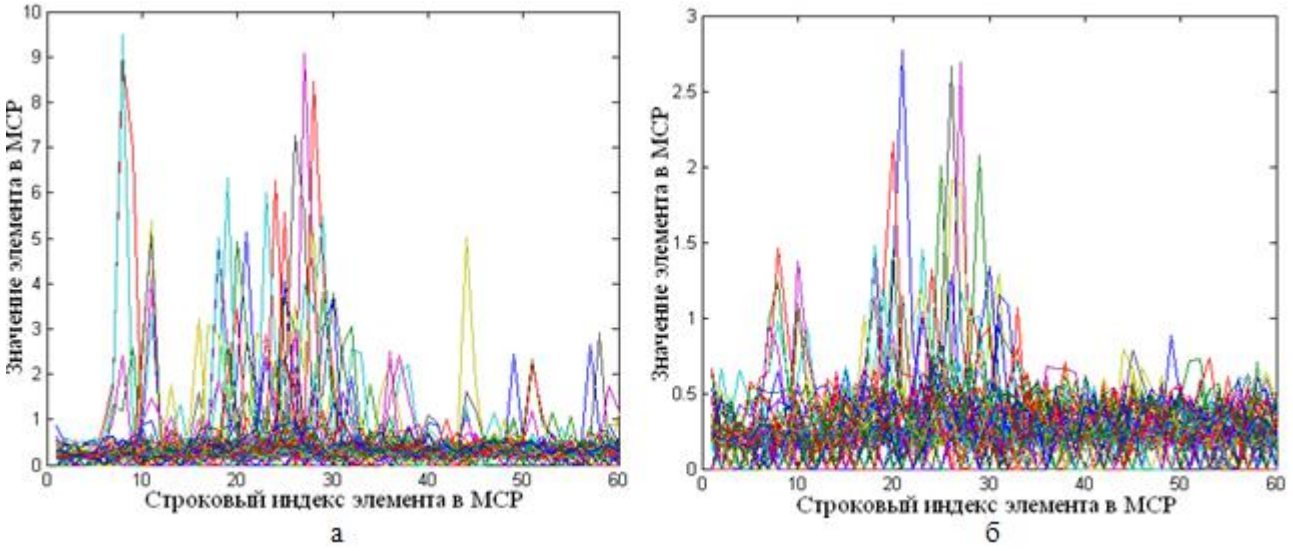


Рис.13.15. РС для тестового ЦЗ в форматі jpeg з $Q = 8$,: а – до розмиття; б – після розмиття (радіус – 1 піксель)

Розмиємо навмисно тестуєме ЦЗ з радіусом 1. Аналізовані характеристики представлені на рис. 13.14(б), 13.15(б). Спостерігаємо аналогічний результат - після проведеного розмиття ДЗ РС зменшився більш ніж в 3 рази. Приблизно в 2 рази зменшився параметр $VMV_{\max}$. Таким чином, вхідне фото не було розмито.

Для оцінки ефективності алгоритму відокремлення РЦЗ від НРЦЗ проведений обчислювальний експеримент, в якому було задіяно більше 1000 ЦЗ в форматі jpeg (з різним параметром «якість»), отриманих сучасними фотокамерами, які зазнали операції РЗ з радіусом 1 у середовищі Photoshop. Результати експеримента наведені в таблиці 13.3.

Таблиця 13.3 — Ефективність алгоритму відокремлення РЦЗ від НРЦЗ (%)

Коефіцієнт якості	$Q = 10$	$Q = 8$
Ефективність без додаткової перевірки	90-95	80-86
Ефективність при використанні додаткової перевірки	99	95

3. Формальне представлення корекції яскравості

Найбільш відомими й широко використовуваними в області обробки зображення колірними моделями є колірна модель RGB і YUV (YIQ). У моделі RGB координатними осями є три первинні кольори: червоний (R), зелений (G) і синій (B), інтенсивність кольору, що змішується, змінюється в діапазоні [0; 255]. Колірні моделі YUV (YIQ), є стандартом передачі інформації, не пов'язані з устаткуванням. У моделі YUV координатними осями є: яскравість (Y) і колірні складові (U = G – R, V = G - B). Як і в моделі RGB інтенсивність кожного колірного компонента змінюється в діапазоні [0; 255].

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.522 & 0.311 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix},$$

де R, G, B – значення інтенсивності червоної, зеленої й синьої складової відповідно.

Таким чином, тут будемо використовувати цифрові зображення, представлені або матрицями R,G,B, або в виді матриці Y (компонента Y містить вхідне зображення в градаціях сірого).

Матричне представлення корекції яскравості ЦЗ з деяким допущенням має такий вигляд:

$$\overline{Y} = Y \pm K,$$

де Y, $\overline{Y}$ – $n \times n$–матриці яскравості ЦЗ до й після корекції відповідно, K – $n \times n$–матриця корекції:

$$K = \begin{pmatrix} k & \dots & k \\ \dots\dots\dots\dots \\ k & \dots & k \end{pmatrix}, \qquad (13.11)$$

де k - натуральне число, що визначає кількість градацій яскравості, на яку відбувається корекція.

На практиці мала частина елементів матриці $\overline{Y} - Y$ можуть незначно відрізнятися від k. Це відбувається в результаті переведення ЦЗ з одного формату зберігання в інший (з метою формування матриці яскравості) у ході виконання операції корекції в графічному редакторі, а також у тому випадку, коли в результаті корекції яскравості елементи $\overline{Y}$ виходять за межі множини $[0,255]$. У силу незначності відмінності на практиці $\overline{Y} - Y$ від K нижче в теоретичних викладеннях ця відмінність не враховується.

Побудуємо для матриці K нормальне сингулярне розкладання:

$$K = U_K \Sigma_K V_K^T,$$

де U_K, V_K - ортогональні матриці лівих (лексикографічно додатних) і правих СНВ відповідно, $\Sigma_K = diag(\sigma_1^K, \dots, \sigma_n^K)$ - матриця СНЧ K.

В силу (13.11):

$$\sigma_1^K > 0, \quad \sigma_2^K = \dots = \sigma_n^K = 0. \qquad (13.12)$$

Одним з найбільш важливих числових параметрів, що характеризують ЦЗ, є енергія E сигналу. Враховуючи різні способи обчислення енергії (для n×n-матриці F з елементами $f_{ij}, i, j = \overline{1,n}$, і СНЧ $\sigma_i, i = \overline{1,n}$, $E = \sum_{i,j} f_{ij}^2 = \sum_i \sigma_i^2$ (лекція 5-6 формула (5.1)) і співвідношення (13.12), для K маємо:

$$E = k^2 n^2 = \left(\sigma_1^K\right)^2,$$

звідки:

$$\sigma_1^K = k \cdot n.$$

Нехай нормальне сингулярне розкладання матриці яскравості Y ЦЗ

$$Y = U \Sigma V^T, \qquad (13.13)$$

де матриці $U=(u_1,...\mu_n)$, $\Sigma=diag(\sigma_1,...,\sigma_n)$, $V=(v_1,...,v_n)$ ($u_i, v_i, i=\overline{1,n}$, - стовпці матриць U,V - ліві і праві СНВ Y).

Відомо, що лівий і правий СНВ матриці Y, що відповідають максимальним СНЧ σ_1, близькі до $n-$оптимального вектора n^O простору R^n. Можна показати, що лівий і правий СНВ матриці K, що відповідають максимальним СНЧ σ_1^K, точно дорівнюють n^O.

Тоді можна вважати, що:

$$\overline{Y}=Y\pm K=U\Sigma V^T\pm U_K\Sigma_K V_K{}^T\approx$$

$$\approx\begin{pmatrix}n^O & u_2 & \dots & u_n\end{pmatrix}\begin{pmatrix}\sigma_1 & 0 & \cdots & 0\\ 0 & \sigma_2 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \sigma_n\end{pmatrix}\begin{pmatrix}n^O & v_2 & \dots & v_n\end{pmatrix}^T\pm$$

$$\pm\begin{pmatrix}n^O & u_2{}^K & \dots & u_n{}^K\end{pmatrix}\begin{pmatrix}kn & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 0\end{pmatrix}\begin{pmatrix}n^O & v_2{}^K & \dots & v_n{}^K\end{pmatrix}^T=$$

$$=\begin{pmatrix}n^O & u_2 & \dots & u_n\end{pmatrix}\begin{pmatrix}\sigma_1\pm kn & 0 & \cdots & 0\\ 0 & \sigma_2 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \sigma_n\end{pmatrix}\begin{pmatrix}n^O & v_2 & \dots & v_n\end{pmatrix}^T \qquad (13.14)$$

Формула (13.14) представляє із себе нормальне сингулярне розкладання матриці $\overline{Y}$, з якої випливає:

— формальним представленням корекції яскравості ЦЗ є збільшення/зменшення у випадку освітлення/затемнення зображення максимального СНЧ σ_1 матриці Y на величину, що дорівнює kn, при цьому всі інші СНЧ залишаються без зміни. Таким чином, визначення кількості градацій яскравості, на яку відбулася корекція, практично може бути проведене відповідно до формули:

$$\overline{k}=\frac{\left|\sigma_1-\overline{\sigma}_1\right|}{n}$$

де $\overline{\sigma}_1$ - максимальне СНЧ матриці $\overline{Y}$;

— СНВ, що є результатом нормального сингулярного розкладання матриці яскравості ЦЗ, у результаті корекції яскравості не змінюються.

Таким чином, при формальному представленні корекції яскравості ЦЗ задіяними є тільки СНЧ відповідних матриць.

2.3. Формальне представлення корекції кольору цифрового зображення

Матричне представлення корекції кольору ЦЗ з деяким допущенням має такий вигляд:

$$\overline{F} = k' F,$$

де F, $\overline{F}$ - $n \times n$-матриці колірного каналу ЦЗ до й після корекції відповідно, k' - скалярне значення корекції, або коефіцієнт корекції, $0 < k' \le 1$.

Нехай сингулярне розкладання матриці будь-якого колірного каналу RGB ЦЗ має вид (13.13).

Тоді:

$$\overline{F} = k' F = k' U \Sigma V^T = U\left(k' \Sigma\right) V^T = U \begin{pmatrix} k'\sigma_1 & 0 & \cdots & 0 \\ 0 & k'\sigma_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k'\sigma_n \end{pmatrix} V^T. \qquad (13.15)$$

З формули (13.15), яка представляє із себе сингулярне розкладання матриці $\overline{F}$, випливає:

— СНЧ $\overline{\sigma}_1, \overline{\sigma}_2, \ldots, \overline{\sigma}_n$ матриці $\overline{F}$ визначаються як:

$$\overline{\sigma}_i = k' \sigma_i, i = \overline{1,n},$$

що є формальним представленням корекції кольору ЦЗ;

— визначення коефіцієнта корекції кольору k' проводиться відповідно до формули:

$$k' = \frac{\overline{\sigma}_1}{\sigma_1} = \frac{\overline{\sigma}_2}{\sigma_2} = \ldots = \frac{\overline{\sigma}_n}{\sigma_n}; \qquad (13.16)$$

— СНВ матриці ЦЗ в результаті корекції кольори не змінюються.

У силу особливостей машинної арифметики при роботі з дійсними числами формула (13.16) на практиці може не виконуватися в точності. Для одержання значення корекції колірного каналу $\overline{k'}$ використовується формула:

$$\overline{k'} = \frac{\overline{\sigma}_1}{\sigma_1}.$$

Таким образом, при формальном представлении коррекции цвета ЦИ задействованными оказываются вновь лишь СНЧ соответствующих матриц, СНВ не принимают участия в указанном процессе.

Питання

1. Як визначаэться нормований вектор СНЧ блоку?
2. Коли порушником використовуэться спотворення ЦЗ шляхом накладання шуму?
3. Якій умові задовольняє більшість $l \times l$ – блоків, отриманих шляхом стандартної розбивки матриці, оригінальних ЦЗ?

4. Для яких блоків зображення має місце рівність $\angle\left(u_1,\overline{\overline{\sigma}}\right)=\angle\left(n^o,e_1\right)$? Пояснити.
5. Блоки якого розміру використовуються в методі виявлення результатів накладання шуму на ЦЗ? Пояснити.
6. Влстивості СНЧ блоків розмитого ЦЗ. Пояснити.
7. Формальне представлення корекції яскравості ЦЗ.
8. Визначення кількості градацій яскравості, на яку відбулася корекція ЦЗ.
9. Формальне представлення корекції кольору цифрового зображення.

Література

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
2. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.
3. Бобок І.І. Теоретичні основи методу виявлення порушення цілісності цифрового зображення в результаті накладання шуму. Збірник наукових праць ВІКНУ імені Тараса Шевченка. 2019. 63. С. 73–84.
4. О.Ю. Лебедєва, В.В. Зоріло, О.А. Карпова. Виявлення «Розумного розмиття» як порушення цілісності цифрового зображення. ІМММ. – 2020. – Т.10, №1-2. – С. 61-67.
5. В.В. Зоріло, О.Ю. Лебедєва, Н.О. Бензар. Розробка алгоритму виявлення зашумлення як фальсифікації цифрового зображення. – ІМММ. – 2021. – Т.11, №1-2.
6. В.В. Зоріло, О.А. Карпова. Алгоритм виявлення обробки цифрового зображення фільтром «Motion blur». – ІМММ, 2019. – Т.9, №1-2. – С. 49-58.

Лекція 14. МЕТОДИ ДЕТЕКТУВАННЯ ФОТОМОНТАЖУ ТА КЛОНУВАННЯ, ЗАСНОВАНІ НА ЗАГАЛЬНОМУ ПІДХОДІ ДО АНАЛІЗУ ІНФОРМАЦІЙНИХ СИСТЕМ

План

1. Фотомонтаж, клонування в цифровому зображенні
2. Матриця найменших сингулярних чисел блоків та її властивості в умовах фотомонтажу F-1
3. Властивості МНСБ у випадку ЦЗ в форматі з втратами

1. Фотомонтаж, клонування в цифровому зображенні

На практиці порушення цілісності ЦЗ часто відбувається локально, у межах якоїсь (невеликої) області, не змінюючи ніяк інші його частини. Такі локальні зміни відбуваються, як правило, внаслідок фотомонтажу або клонування.

Під фотомонтажем розуміється заміна частини (частин) одного ЦЗ, що будемо називати основним (ОЗ), частиною (частинами), що будемо називати заміщуючою областю (ЗО), або вклейкою, іншого ЦЗ (рис.14.1).

а б в

Рис.14.1. Ілюстрація застосування для ЦЗ фотомонтажу: а, б – оригінальні ЦЗ; в – результат проведеного фотомонтажу

Клонування - одна з операцій, яка найчастіше використовується при фальсифікації ЦЗ та реалізується всіма графічними редакторами. В ході клонування відбувається заміна частини (частин) ЦЗ, частиною (частинами) того ж ЦЗ. В отриманому результаті області, що змінилися, називаються клонованими (клонами), або образами оригінальних, а оригінальні області, що послужили основою для клонів, називаються їх прообразами (рис.14.2).

а б

Рис.14.2. Ілюстрація застосування для ЦЗ клонування: а – оригінальне ЦЗ; б – результат проведеного клонування

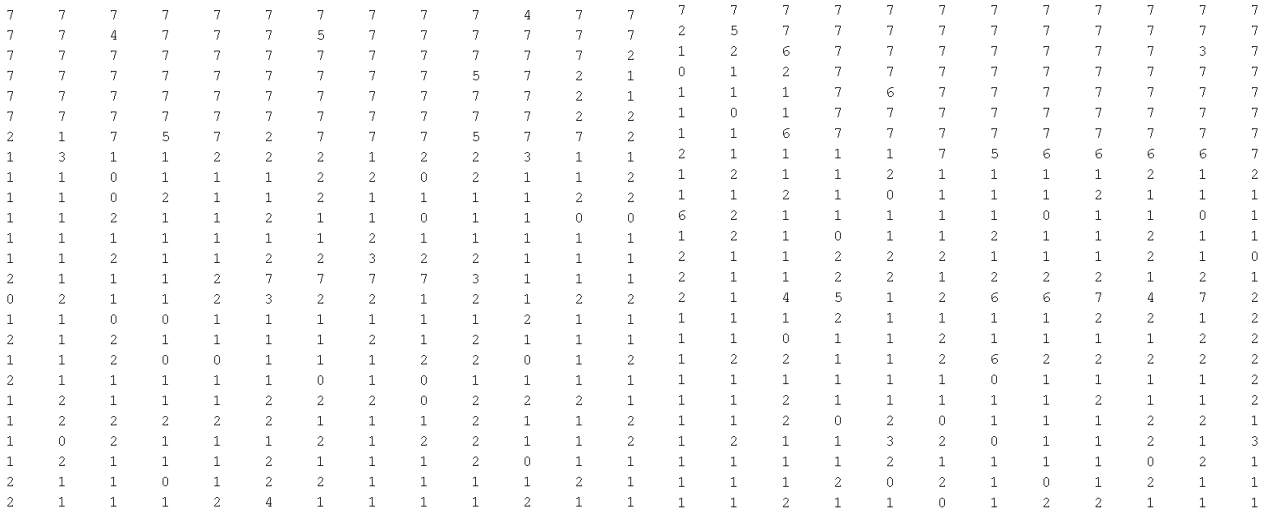
І якщо розв'язок питання виявленням фотомонтажу чітко вказує на область порушення цілісності, то в результаті виявлення результатів клонування визначаються області клону й прообразу, причому, як правило, без відокремлення однієї від іншої. Але в останньому випадку порушення цілісності відбувається локально лише в області клону (при відсутності якої-небудь додаткової обробки ЦЗ), а область прообразу залишається оригінальною, тому виявлення порушення цілісності тут – це не тільки визначення областей клону й прообразу, але й відокремлення однієї від іншої. І якщо задачі виявлення областей клону й прообразу приділяється багато уваги в сучасному науковому світі, то друга задача в силу своєї складності залишається маловивченою.

2. Матриця найменших сингулярних чисел блоків та її властивості в умовах фотомонтажу F-1

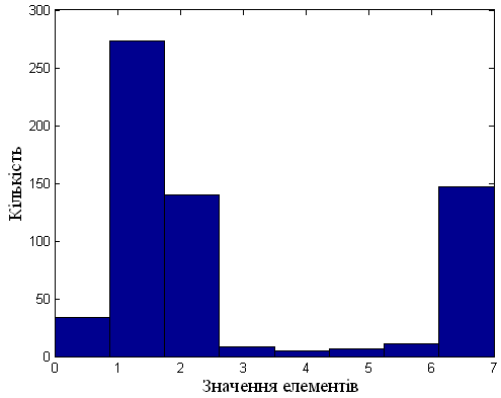
Нехай основне зображення - ЦЗ в форматі з втратами, ЗО – ЦЗ в форматі без втрат. Для більшої наочності демонстрації основної ідеї виявлення фотомонтажу вважаємо, що ніяка наступна обробка зображення не проводиться. Фальсифіковане зображення (фотомонтаж) зберігається без втрат. Таку процедуру фотомонтажу далі будемо позначати F-1.

Назвемо матрицею найменших СНЧ блоків (МНСБ) матрицю, кожний елемент якої визначає кількість СНЧ у відповідному блоці, менших заданого порога T. Очевидно, що МНСЧ для ЦЗ у різних форматах зберігання (з/без втрат) будуть відрізнятися друг від друга (рис.14.3 - T=0.5): для блоків ЦЗ в форматі без втрат їх, як правило, менше, ніж в блоках ЦЗ в форматі з втратами, на що наочно вказують гістограми МНСБ (рис.14.3 (в,д)).

а

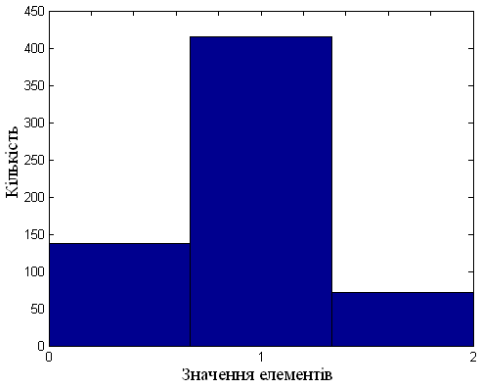


б



В

Г

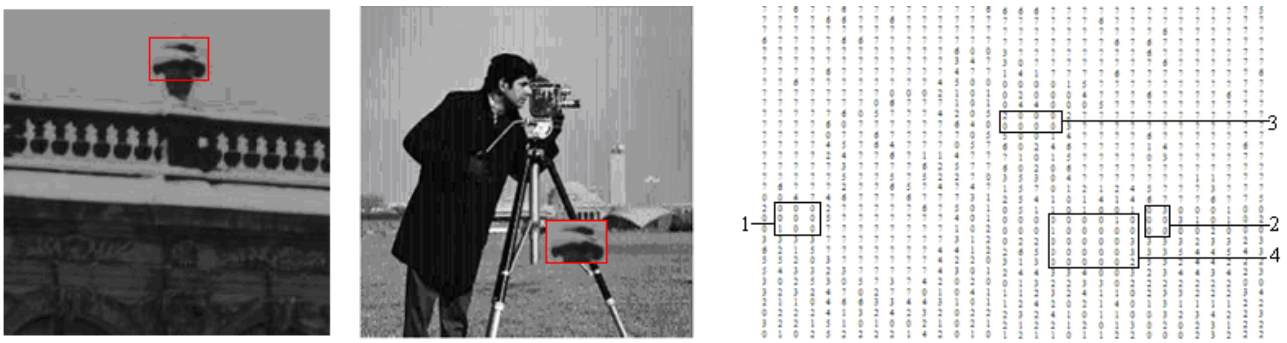


Д

Рис.14.3. а – ЦЗ1 розміром 200*200 пікселів в форматі Jpeg QF=75; б – МНСБ для ЦЗ1; в – гістограмма значень МНСБ для ЦЗ1; г - МНСБ для ЦЗ2 в форматі Tif, відповідного ЦЗ1; д - гістограмма значень МНСБ для ЦЗ2

При побудові МНСБ отриманого фотомонтажу частини, що відповідають ОЗ й ЗО, будуть відрізнятися по кількості найменших СНЧ блоків, менших порога Т: підобласть МНСБ, яка відповідає вклейці, буде містити велику кількість нулів і значень, що мало відрізняються від нуля (на рис.14.4(в) ця частина виділена під номером 4).

Для детектування ЗО необхідно виділити в МНСБ зв'язні області, що містять нулі й близькі до нуля значення. Такі сукупності можуть відповідати: а) вклейкам, б) областям ОЗ, що містять контури. На рис.14.4(в) приклади областей б) виділено під номерами 1,2,3.



а б в

Рис.14.4. а – ЦЗ в форматі без втрат, що використовувалося для фотомонтажу; б – фальсифіковане ЦЗ, де ОЗ зберігалося в форматі з втратами; в – МНСЧ для фальсифікованого ЦЗ

Проведемо Jpeg-стиск для змонтованого зображення, але масив нормалізації (матрицю квантування) оберемо так, щоб його елементи були менше, чим використані при першому квантуванні коефіцієнтів ДКП ОЗ. Друге квантування й відновлення не повинні якісно змінити картину для сингулярних спектрів блоків 1,2,3-ої областей ОЗ. Дійсно, відсутність СНЧ, менших Т, у блоках цих частин, значна відмінність останніх (найменших) СНЧ від нуля говорить про те, що ці блоки містять велику кількість контурів, тобто значними є коефіцієнти ДКП, що відповідають високим і середнім частотам. Якщо ці коефіцієнти не обнулилися при першому квантуванні, то більша їхня частина залишиться ненульовими й при другому, де коефіцієнти квантування будуть менше. Для вклейки процес квантування коефіцієнтів ДКП буде першим, тому проявиться картина результатів першого квантування - значне зменшення значень малих СНЧ у її блоках. Проілюструємо вищесказане на розглянутому прикладі (рис.14.5).

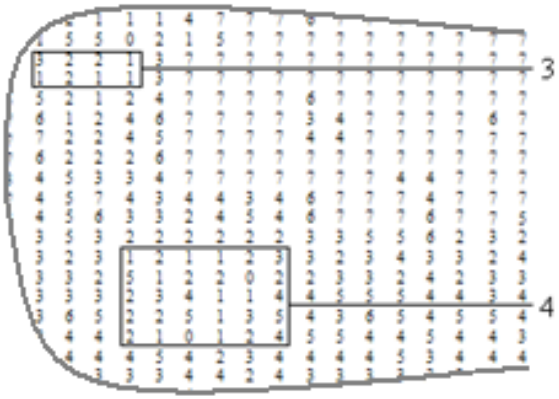


Рис.14.5. Фрагмент МНСБ після Jpeg-стиску змонтованого зображення

При відновленні змонтованого зображення після його Jpeg-стиску, як і очікувалося, для області 3 ОЗ картина кількості малих СНЧ, менших за Т, у блоках змінилася незначно. Для вклейки елементи МНСБ змінилися в діапазоні від 1 до 5 (рис.14.5), що явно відокремить її від області 3 і інших подібних. Зазначимо, що в запропонованому прикладі вклейка сама по собі містить багато контурів, маленьких деталей. Якщо ж вклейка представляє із себе частину зображення з малою кількістю або відсутністю контурів, то відрізнити її від області типу 1-3 ОЗ буде значно легше: елементи МНСБ будуть ще більше відрізнятися від нуля після відновлення зображення.

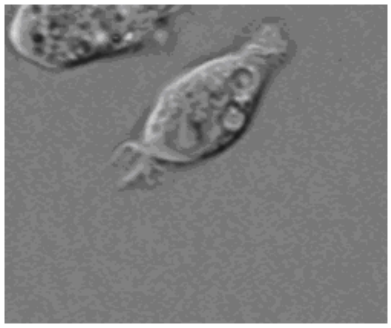
Зауваження. Очевидно, запропонований підхід може використовуватися також у випадку, коли основне зображення зберігається в форматі без втрат, а вклейка є частиною зображення у форматі з втратами.

3. Властивості МНСБ у випадку ЦЗ в форматі з втратами

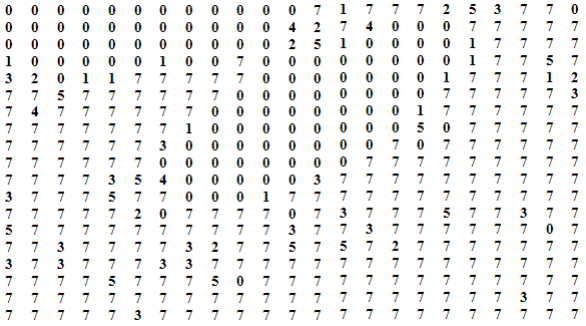
Розглянемо спосіб фотомонтажу, який найбільш часто зустрічається на практиці. Нехай ОЗ і ЗО отримані з ЦЗ в форматі з втратами (Jpeg).

Після здійснення фотомонтажу зображення знову зберігається у форматі Jpeg. Це приводить до повторного квантування коефіцієнтів ДКП, при цьому матриця квантування може бути відмінна від використовуваної при першому квантуванні. Такий спосіб фотомонтажу для зручності викладу будемо називати нижче F-2.

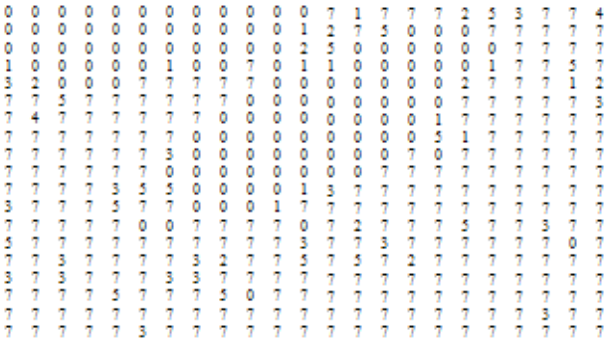
Розглянемо докладно на прикладі зображення Cell (рис.14.6) типові зміни, що відбуваються з СНЧ блоків при повторному квантуванні коефіцієнтів ДКП для повністю відновленого після першого квантування зображення, де елементи матриці повторного квантування можуть бути відмінні від елементів матриці первинного стиску. Зауважимо, що відмінність не може бути значною, оскільки матриці квантування будуються таким чином, щоб урахувати не тільки надлишковості ЦЗ з метою його стиску, але й особливості зорової системи людини для забезпечення відсутності артефактів на зображенні після його відновлення.



а



б



в

Рис.14.6. а – подане ЦЗ в форматі Jpeg; б – відповідна МНСБ; в – МНСБ після повторного стиску

Використовується стандартна розбивка матриці зображення на блоки як при першому, так і при другому квантуванні. МНСБ, що отримуються після одного й двох квантувань, будуть мало відрізнятися друг від друга, однак важливим фактором тут є збіг сіток розбивки на блоки (СРБ) матриці ЦЗ при першому й другому квантуванні.

Розглянемо варіант, коли згадані сітки різні. Зміна розташування сітки може привести до зміни рангів матриць блоків. Дійсно, нехай відбувся зсув сітки на одну позицію вправо. Цей зсув виключить із конкретного блоку один (перший) стовпець і додасть новий, який виявиться останнім. Введений стовпець, що спочатку належав іншому блоку, сформований при його квантуванні, як правило, виявляється лінійно незалежним зі стовпцями блоку, у

якому він опинився. Якщо при цьому виключений перший стовпець був одним з тих, які визначали ранг блоку, то описаний зсув СРБ не змінить рангу матриці. А якщо ні, то, ранг матриці блоку збільшиться на 1, що очікувано приведе до зменшення кількості СНЧ, менших порога T, на 1. Оскільки ранг матриці визначається не тільки лінійно незалежними стовпцями, але й рядками, то все сказане вище буде мати місце й у тому випадку, якщо зсув сітки здійснюється на одну одиницю вниз. Одночасний зсув по обом осям також, як правило, приведе до незменшення рангів матриць блоків. Якщо зсув сітки відбувається не тільки по обом осям, але й на кількість одиниць, більше 1, то, на перший погляд, нічого конкретного про зміну елементів МНСБ сказати не можна: стовпці(рядки), що підключаються/виключаються, і їх частини можуть бути як лінійно залежними, так і визначати ранг. Однак, беручи до уваги, що для випадково обраних m векторів з простору вимірності n, де $m<n$ (в нашому випадку $m \le 4,\ n=8$), імовірність того, що вони виявляться лінійно залежними менше, чим імовірність того, що вони виявляться лінійно незалежними, логічно припустити, що в більшості випадків при описаній вище операції зсуву сітки це знову повинно привести до незменшення рангу матриці. Обчислювальний експеримент, проведений у середовищі Matlab, підтверджує незбільшення елементів МНСБ при зсуві сітки, однак їх зменшення в загальному випадку, як і було відзначено вище, непередбачене, приводить до значного розкиду значень елементів МНСБ - від 1 до 7, що є характерною рисою неспівпадіння сіток первинної і вторинної розбивки матриці (рис.14.7).

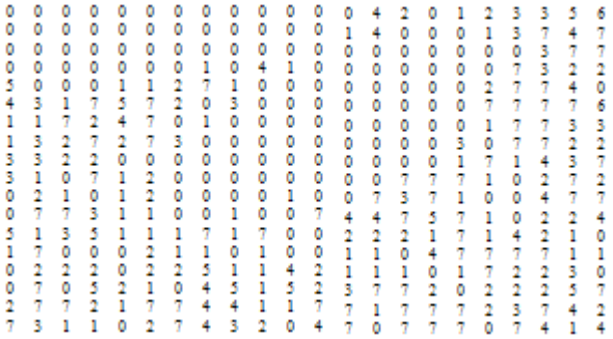


Рис.14.7. МНСБ при зсуві СРБ на 2 по осях ОХ і ОУ

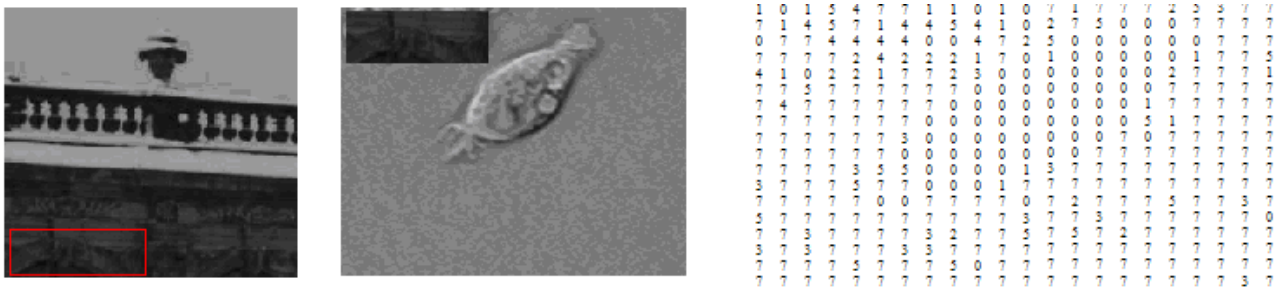
Зауважимо однак, що згадане зменшення й розкид значень елементів МНСБ характерний для областей, що відповідають фоновим частинам вхідного зображення. Що стосується підобластей, що містять численні контури, то вони практично залишаються незмінними при зсуві сітки дискретизації: кількість СНЧ, менших T, таких блоків невелика спочатку, зсув сітки з великою ймовірністю не змінює картину лінійної незалежності стовпців (рядків) матриць блоків, оскільки, ті, що виключаються із блоку, що підключаються до блоку, стовпці (рядки) або їх частини лінійно незалежні.

Інтерес до поведінки елементів МНСБ при зміні положення сітки розбивки матриці ЦЗ невипадковий. Якщо фотомонтаж здійснюється так, як передбачалося вище, тобто ОЗ й ЗО є результатами одинарного квантування (з однією або різними матрицями квантування), то ймовірність збігу сіток розбивок ОЗ й ЗО після здійснення фотомонтажу мала, а значить особливості МНСБ, що виникають за рахунок такої розбіжності, укажуть на наявність фальсифікації.

Скористаємося особливістю СНЧ при повторному квантуванні з незбіжними СРБ для виявлення фотомонтажу F-2.

Для наочності викладу розглянемо приклад. ЦЗ Cell збережене в форматі Jpeg. На його основі формується фотомонтаж Cell1, представлений на рис.14.8. Сітки розбивок ОЗ й ЗО при первинному стиску після здійснення фотомонтажу не співпадають. Якщо отриманий фотомонтаж знову зберегти у форматі Jpeg, що приведе до повторного квантування

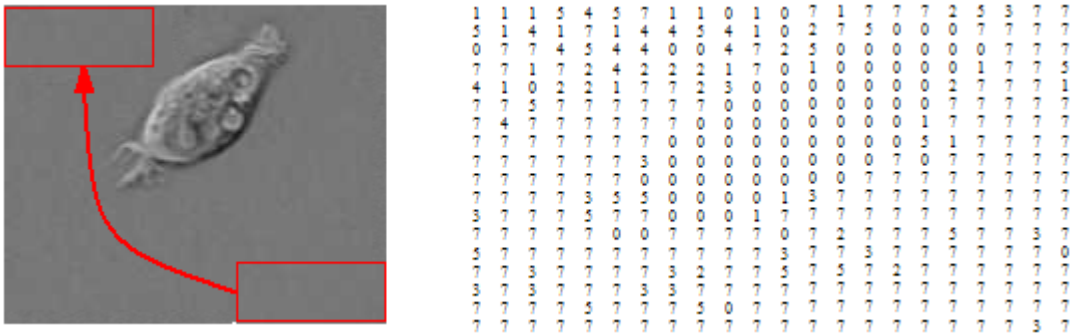
коефіцієнтів ДКП, що припускає F-2, беручи для цього сітку розбивки стандартним чином (вона співпаде із сіткою першого квантування тільки для ОЗ й не співпаде для ЗО), то МНСБ буде виглядати так, як представлено на рис.14.8(в). Увага привертає підобласть МНСБ, розташована в її лівому верхньому куті, де без усякого «порядку» локалізовані значення від 0 до 7, що і виділяє область вклейки.



а б в

Рис.14.8. а – ЦЗ, що було використаним при фотомонтажі (формат Jpeg); б – результат фотомонтажу – ЦЗ CELL1; в – МНСБ після стиску CELL1

Аналогічні властивості має МНСБ у випадку клонування при неспівпадінні сіток розбиття на блоки при первинному і повторному стиску для області клону (рис.14.9).



а б

Рис.14.9. а – клоноване ЦЗ і збережене в форматі з втратами (Jpeg); б – МНСБ для клонованого ЦЗ

Таким чином, дослідження властивостей матриці МНСБ дає можливість отримати таки її характерні риси, які дозволяють ефективно виявляти області локальних порушень цілісності ЦЗ.

Питання

a. Що таке фотомонтаж, клонування? Чим принципово фотомонтаж відрізняється від клонування?
b. Що таке матриця найменших сингулярних чисел блоків? Для чого вона використовується?
c. Для ЦЗ у якому форматі (з/без втрат) МНСБ є більш інформативною? Чому? Яку інформацію ми можемо отримати з неї?
d. Властивості МНСБ у випадку ЦЗ в форматі з втратами. Пояснити.
e. Як матриця найменших сингулярних чисел блоків використовується в умовах фотомонтажу F-1, клонуванні? Роль сіток розбивки.

Література

2. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.

3. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.
4. Хорошко В.О., Бобок І.І. Аналіз особливостей удосконаленого загального підходу до проблеми виявлення порушень цілісності цифрових зображень. Сучасна спеціальна техніка. 2019. 2(57). С. 59–71.
5. Хорошко В.О., Бобок І.І. Виявлення локального порушення цілісності цифрового зображення. Інформатика та математичні методи в моделюванні. 2019. 9(1-2). С. 24–37.
6. Bobok I.I., Kobozeva A.A., Grygorenko S.M. Method for detecting of clone areas in a digital image under conditions of additional attacks. Journal of Signal Processing Systems. 2020. 92. P. 55–69. [SCOPUS]
7. Хорошко В.О., Бобок І.І. Удосконалення методу виявлення результатів клонування в цифровому зображенні. Вісник ЧДТУ: Технічні науки. 2019. 3. С. 38–49.
8. **Nor Bakiah AbdWarif, Ainuddin Wahid AbdulWahab, Mohd Yamani Idnaldris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, Kim-Kwang Raymond Choo. Copy-move forgery detection: Survey, challenges and future directions. Journal of Network and Computer Applications**. **Volume 75**, 2016, Pages 259-278. **https://www.sciencedirect.com/science/article/abs/pii/S1084804516302144**
9. Hui-Yu Huang, Ai-Jhen Ciou. Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. **EURASIP Journal on Image and Video Processing volume** 2019, Article number: 68 (2019). **https://jivp-eurasipjournals.springeropen.com/articles/10.1186/s13640-019-0469-9**
10. Esteban Alejandro Armas Vega, Edgar González Fernández, Ana Lucila Sandoval Orozco, Luis Javier García Villalba. Copy-move forgery detection technique based on discrete cosine transform blocks features. **Neural Computing and Applications volume** 33, **pages** 4713–4727 (2021). **https://link.springer.com/article/10.1007/s00521-020-05433-1**
11. Бобок І.І., Кобозєва А.А. Теоретичні основи методу відокремлення клону від прообразу в цифровому зображенні. Безпека інформації. 2018. 24(1). С. 49–55. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=bezin_2018_24_1_9
12. Бобок І.І., Кобозєва А.А. Метод відокремлення клону від прообразу в цифровому зображенні в умовах відсутності постобробки зображення. Вісник ЧДТУ: Технічні науки. 2018. 2. С. 12–19. http://vtn.chdtu.edu.ua/article/view/161847

Лекція 15. ВИЯВЛЕННЯ ЛОКАЛЬНОГО ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ В УМОВАХ КЛОНУВАННЯ

План

1. Два підходи, що застосовуються для відокремлення клону від прообразу
2. Теоретичні основи відокремлення клону від прообразу в цифровому зображенні в умовах відсутності відмінностей в їх постобробці
3. Метод відокремлення клону від прообразу в умовах відсутності постобробки зображення

1. Два підходи, що застосовуються для відокремлення клону від прообразу

Існуючі нечисленні методи для розв'язку задачі відокремлення клону від прообразу, інформація про які є доступною з відкритих джерел, ґрунтуються на двох принципово різних підходах до організації такого відокремлення.

Перший підхід ґрунтується на використання цифрових водяних знаків (ЦВЗ). Він був використаний при розробках методу виявлення порушень цілісності цифрового зображення шляхом використання стеганографічних алгоритмів, а також методу виявлення результатів клонування з наступним відокремленням області клону від області прообразу в ЦЗ в умовах відсутності відмінностей у постобробці (якщо вона має місце) областей клону й прообразу. Вбудова ЦВЗ здійснювалася тут стійкими до атак проти вбудованого повідомлення стеганоалгоритмами. Перший підхід дозволив ефективно відокремлювати клон від прообразу, але на формальному рівні процес вбудови ЦВЗ сам по собі порушує цілісність оригінального зображення, тому такий підхід не може бути пріоритетним.

Другий підхід базується на виявленні відмінностей у результатах обробки клону й прообразу. Але якщо розміри клону малі, то його додаткова обробка буде відсутньою, чи клон і прообраз можуть оброблятися однаково, наприклад, при стиску ЦЗ з втратами.

Таким чином, задача відокремлення клону від прообразу залишається до кінця невирішеною й актуальною, зокрема, для областей малих розмірів та в умовах відсутності обробки чи різниці при (довільній) обробці клону і прообразу, для яких в відкритих джерелах не знайдено методів її розв’язку.

Існуючі методи, як правило, працюють з областями клону/прообразу, площа яких більша 1% від загальної площі ЦЗ (площі визначаються кількістю пікселів, що потрапили у відповідну область), рідко пропонуються методи, що визначають обговорювані області, коли їх площі менше, чим 1% площі всього ЦЗ.

Будемо вважати, що ЦЗ, що зазнало клонування, виявлене як клоноване, якщо визначені області клону і прообразу мають непусте перетинання з реальними клоном і прообразом.

2 Теоретичні основи відокремлення клону від прообразу в цифровому зображенні в умовах відсутності відмінностей в їх постобробці

Далі припускається, що області клону й прообразу в ЦЗ виявлені на попередньому етапі в результаті роботи відповідного алгоритму.

Розглянемо як неоригінальну область ЦЗ клон. При клонуванні відбувається «розрив зв'язків» між сусідніми пікселями для області клону (пікселями, що лежать на границі області), а для області прообразу нічого не зміниться. Розрив існуючих зв'язків з врахуванням всього вищевикладеного з великою ймовірністю приведе до того, що для клону, який замінить собою оригінальну область ЦЗ, відмінність між значеннями його граничних пікселів і пікселів, що є тепер безпосередніми сусідами, але належать оригінальній частині ЦЗ, буде більше, ніж між відповідними їм пікселями прообразу і їх безпосередніми сусідами в оригінальній області ЦЗ.

Для спрощення викладу припустимо, що клону й прообразу відповідають по одному $l \times l$-блоку $\overline{B}$ і $\overline{\overline{B}}$, для яких невідомо, де саме клон, а де прообраз. Назвемо ***відмітним околом*** довільного блоку B ЦЗ радіуса k $(2k+1)\times(2k+1)$-матрицю, елементи якої

відображають відмінність B від блоків ЦЗ, що знаходяться від B на відстані, що не перевищує k. При цьому сусідами блоку B, що знаходяться від нього на відстані k, назвемо блоки ЦЗ, місця розташування яких отримуються шляхом зсуву B на k пікселів вправо, вліво, вгору, вниз, вздовж головної й побічної діагоналей (вгору, вниз). Так блок, що не лежить на границі ЦЗ, має 8 сусідів на відстані 1 та максимально 16 сусідніх блоків на відстані 2.

Оскільки кореляція значень яскравості найбільше проявляється для пікселів, для яких відстань між ними дорівнює 1, і значно знижується навіть при мінімальному збільшенні p, а також для рядків/стовпців матриці ЦЗ (блоку матриці), що стоять поруч (сусідніх), то норма відмітного околу малого радіуса блоку-клону повинна бути більше норми відмітного околу відповідного блоку-прообразу того ж радіуса у випадку, якщо клон і прообраз не обробляються або обробляються однаково, що дозволить відокремити клон від прообразу у таких умовах.

Для перевірки на практиці висунутої гіпотези був проведений обчислювальний експеримент, у якому були задіяні 500 ЦЗ із бази NRCS. Оскільки передача інформації (ЦЗ, цифрові відео, аудіо) у даний момент по каналах зв'язку відбувається у форматах з втратами (ФзВ), то ЦЗ після того, як воно піддалося клонуванню, з великою долею ймовірності буде збережено у ФзВ, що певним чином змінить зображення й є одним зі способів його постобробки після клонування. Таким чином, можна вважати, що на практиці ЦЗ після клонування часто буде піддаватися постобробці, але ця постобробка не буде відрізнятися для областей клону й прообразу.

У ході експерименту оригінальні цифрові зображення піддавалися клонуванню, де як прообраз використовувався $l \times l$ - блок, $l \in \{8, 16, 24, 32\}$, після чого клоноване ЦЗ зберігалося у форматі без втрат (Tif) або піддавалося додатковим збурним діям (постобробці), у якості яких, в першу чергу, розглядався стиск із втратами (збереження у форматі Jpeg з різними коефіцієнтами якості QF) (результати відображені в табл. 15.1). Також в експерименті задіювалося накладання різних шумів з різними параметрами, комплексні збурні дії. Для отриманих таким чином цифрових зображень області клону й прообразу вважалися вже виявленими – $\overline{B}$ і $\overline{\overline{B}}$. Кожному з блоків $\overline{B}$ і $\overline{\overline{B}}$ ставилися у відповідність відмітні околи цих блоків $\overline{O}^{(1)}, \overline{\overline{O}}^{(1)}$ (радіуса 1) і $\overline{O}^{(2)}, \overline{\overline{O}}^{(2)}$ (радіуса 2) відповідно. Очевидно, що $\overline{O}^{(1)}\left(\overline{\overline{O}}^{(1)}\right)$ є підматрицею $\overline{O}^{(2)}\left(\overline{\overline{O}}^{(2)}\right)$.

Відмінність між будь-якими блоками $B^{(1)}, B^{(2)}$ ЦЗ визначалася в сенсі величини: $\sum_{t,p=1}^{l} r_{tp}$, де $r_{tp}, t, p = \overline{1,l}$, — елементи $l \times l -$ матриці $R = \left|B^{(1)} - B^{(2)}\right|$.

Для блоків $\overline{B}$ і $\overline{\overline{B}}$ у ході експерименту обчислювалися норми $\overline{O}^{(1)}, \overline{\overline{O}}^{(1)}$. Клоном вважався той блок, норма відмітного околу якого була більше. Аналогічні дії робилися для $\overline{O}^{(2)}, \overline{\overline{O}}^{(2)}$.

Результати обчислювального експерименту, що підтверджують висунуту гіпотезу, наведені в табл. 15.1, 15.2, де зазначена кількість помилок визначалася відносною кількістю цифрових зображень (вираженою у відсотках від загальної кількості проаналізованих зображень), де клон і прообраз були відокремлені не вірно.

Як показують результати обчислювального експерименту, використання як числового параметру норми відмітного околу попередньо виявлених блоків клону/прообразу дозволяє ефективно відокремлювати ці області.

Як і очікувалося, більш інформативним є відмітний окіл блоку радіуса 1 (у табл.15.1,15.2 результати для такого околу виділені жирним шрифтом). З зростанням сили збурної дії кількість помилок при відокремленні клону від прообразу зростає, із збільшенням

розміру клону, прообразу (КП) кількість помилок зменшується, що також знаходиться в повній відповідності з вищесказаним. Запропонований підхід, заснований на оцінці норм відмітних околів, значно знижує свою ефективність у випадку малого розміру клону, прообразу ($l < 8$), оскільки тут різниця в нормах відмітних околів може бути настільки незначною, що не дає змогу ефективно відокремити прообраз від клону.

Таблиця 15.1

Відносна кількість (%) помилок при відокремленні клону від прообразу в умовах збереження клонованого ЦЗ без втрат (Tif), а також з втратами (Jpeg) з різними коефіцієнтами якості (*QF*)

Розмір клону/прообразу		8×8		16×16		24×24		32×32	
k		1	2	1	2	1	2	1	2
Формат збереження клонованого ЦЗ	Tif	2.5	9.5	2	10.5	0.5	8	0	3
	QF=95	2	9	3	11.5	0.5	8	0.5	1
	QF=85	4.5	10	4.5	11	4	7.5	2	3
	QF=75	9.5	14	10.5	15	6.5	11.5	2.5	5
	QF=65	12	16.5	13.5	16.5	7	8.5	4	5.5

Таблиця 15.2

Відносна кількість (%) помилок при відокремленні клону від прообразу в умовах додаткових збурних дій, включаючи комплексні

Розмір клону/прообразу	Додаткова збурна дія на ЦЗ після здійснення клонування															
	Гауссівський шум з нульовим математичним очікуванням								Мультиплікативний шум							
	D=0.0001				D=0.0005				D=0.0005				D=0.001			
	Формат збереження ЦЗ після ЗД				Формат збереження ЦЗ після ЗД				Формат збереження ЦЗ після ЗД				Формат збереження ЦЗ після ЗД			
	Tif		Jpeg (QF=75)		Tif		Jpeg (QF=75)		Tif		Jpeg (QF=75)		Tif		Jpeg (QF=75)	
	k		*k*		*k*		*k*		*k*		*k*		*k*		*k*	
	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
16×16	3	11	7	14	3.5	12	8	15	3	11	7	14	4	12.5	10	15
32×32	0.5	4.5	3.5	6	1	5.5	5.5	7.5	0.5	4	4	6.5	1	5	4	7

3 Метод відокремлення клону від прообразу в умовах відсутності постобробки зображення

Припустимо, що після клонування не робилася ніяка постобробка КП, ЦЗ збережене без втрат. Нехай результатом роботи деякого використаного методу виявлення клонування є виділені області КП в ЦЗ: $\overline{T}, \overline{\overline{T}}$. Будемо вважати, що $\overline{T}, \overline{\overline{T}}$ є підобластями реальних областей $\overline{P}, \overline{\overline{P}}$ клону й прообразу: $\overline{T} \subseteq \overline{P}, \overline{\overline{T}} \subseteq \overline{\overline{P}}$, що відповідає результатам роботи багатьох існуючих для розв'язку цієї задачі методів (ідеальний варіант, якщо $\overline{T} = \overline{P}, \overline{\overline{T}} = \overline{\overline{P}}$).

Назвемо граничним кожний такий піксель області T ЦЗ, будь-який окіл якого (з радіусом $r \in \mathrm{N}$) буде містити такі пікселі, що належать, і такі, що не належать T; внутрішнім будемо називати кожний такий піксель T, для якого існує такий його окіл, який

містить у собі тільки пікселі з області T; внутрішністю області T назвемо сукупність внутрішніх пікселів T (рис.15.1).

Візьмемо пари відповідних $l \times l$-блоків виявлених областей $\overline{T}, \overline{\overline{T}}$ так, щоб вони належали внутрішностям клону й прообразу (рис.15.2). Таких пар може бути не одна. Нехай таких пар обрано $t \in \mathrm{N}$: $\overline{B}^{(1)}, \overline{\overline{B}}^{(1)}$; $\overline{B}^{(2)}, \overline{\overline{B}}^{(2)}$; …; $\overline{B}^{(t)}, \overline{\overline{B}}^{(t)}$.

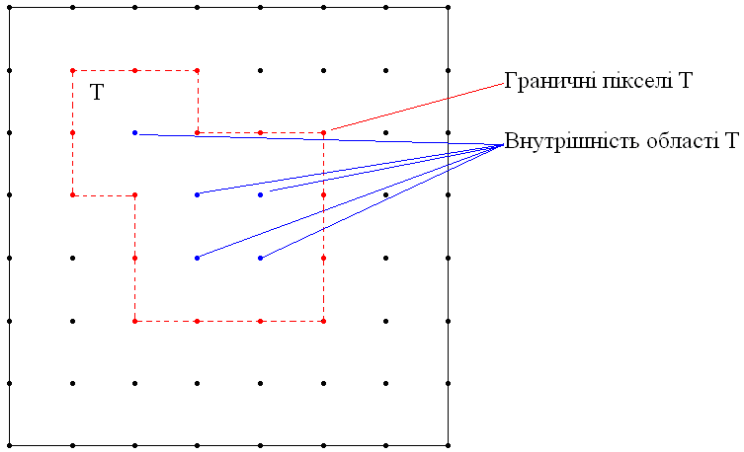


Рис. 15.1. Граничні пікселі, внутрішність області *T* ЦЗ

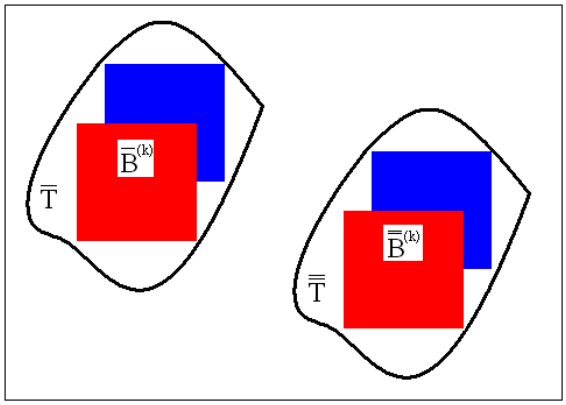


Рис.15.2. Виявлені на ЦЗ області $\overline{T}, \overline{\overline{T}}$ з парами відповідних (однаково пофарбованих) $l \times l$-блоків

Вимога приналежності блоків $\overline{B}^{(k)}, \overline{\overline{B}}^{(k)}$, $k = \overline{1,t}$, внутрішностям $\overline{T}, \overline{\overline{T}}$ має своєю метою забезпечення можливості точного визначення моменту виходу формованих відмітних околів відповідних блоків за межі $\overline{P}, \overline{\overline{P}}$ клону/прообразу. Дійсно, для блоків $\overline{B}^{(k)}, \overline{\overline{B}}^{(k)}$ у випадку, якщо вони є підмножинами внутрішностей $\overline{T}, \overline{\overline{T}}$, то з урахуванням припущення, зробленого вище, вони є підмножинами внутрішностей областей $\overline{P}, \overline{\overline{P}}$. Тоді їх відмітні околи одиничного радіуса очевидно мають однакову норму, оскільки після клонування ЦЗ не зазнало ніякої додаткової обробки. Будемо розглядати тепер пари відповідних блоків ЦЗ, розташування яких відповідає послідовному зсуву $\overline{B}^{(k)}, \overline{\overline{B}}^{(k)}$ на 1, 2, …, p пікселів у довільному напрямку. Доти, поки розглянуті пари будуть відповідати блокам, що

знаходяться у межах внутрішностей $\overline{T},\overline{\overline{T}}$, різниця норм відповідних їм відмітних околів буде дорівнювати 0. Як тільки згадане значення буде відрізнятися від 0, це буде означати, що чергова пара відповідних блоків містить у собі граничні пікселі $\overline{P},\overline{\overline{P}}$, а значить блоки, що є безпосередніми сусідами тих, що розглядаються у даний момент, які використовуються при побудові відмітних околів, містять пікселі, що не належать $\overline{P},\overline{\overline{P}}$. Ці пікселі для пікселів області прообразу є оригінальними сусідами, а для області клону такими, які в оригінальному ЦЗ їх сусідами не є. Все це приведе до того, що відмітний окіл блоку, який відповідає клону, з великою ймовірністю буде мати норму більше, ніж аналогічний окіл для блоку, що відповідає області прообразу, вказуючи на розрив кореляційних зв'язків між значеннями пікселів, що знаходяться поруч в оригінальному ЦЗ, при створенні клону. Ця властивість і є основною для організації процесу відокремлення клону від прообразу в умовах відсутності будь-якої їх постобробки. Тут необхідно відзначити наступне. Момент виходу за межі областей $\overline{P},\overline{\overline{P}}$ пари відповідних блоків $\overline{R}^{(k)},\overline{\overline{R}}^{(k)}$, місце розташування яких відповідає зсуву $\overline{B}^{(k)},\overline{\overline{B}}^{(k)}$ на певну кількість пікселів у певному напрямку, може відбутися при дуже кількісно незначному включенні «сторонніх», тобто таких, що не належать $\overline{P},\overline{\overline{P}}$, пікселів у блоки-сусіди (наприклад, 1-2 пікселя), що використовуються при побудові відмітних околів для $\overline{R}^{(k)},\overline{\overline{R}}^{(k)}$ одиничного радіусу. У цьому випадку відмінність у нормах відмітних околів $\overline{R}^{(k)},\overline{\overline{R}}^{(k)}$ може не вірно вказати на клон у силу того, що відмінності для значень одиничних пікселів оригінальної й неоригінальної областей ЦЗ, загалом кажучи, можна розглядати як випадкову величину, що не дає об'єктивної якісної оцінки співвідношення норм відмітних околів $\overline{R}^{(k)},\overline{\overline{R}}^{(k)}$. Для врахування такої ситуації має сенс проводити порівняння значень відмітних околів відповідних блоків при виході за межі $\overline{P},\overline{\overline{P}}$ не один раз (зсовуючи на початку виділені блоки $\overline{B}^{(k)},\overline{\overline{B}}^{(k)}$ в одному обраному (випадково) напрямку), а кілька разів, досягаючи границі $\overline{P},\overline{\overline{P}}$, рухаючись у різних напрямках щодо первісного положення блоків $\overline{B}^{(k)},\overline{\overline{B}}^{(k)}$ і роблячи висновок про те, яка з $\overline{T},\overline{\overline{T}}$ є клоном, а яка прообразом, залежно від того, яка з цих областей частіше визначалася як клон, а яка як прообраз (з врахуванням усіх розглянутих напрямків зсуву).

У зв’язку з вищесказаним пропонується метод відокремлення області клону від прообразу *KP2*, основні кроки якого наступні.

Крок 1. Нехай $\overline{T},\overline{\overline{T}}$ – виявлені попередньо в ЦЗ області клону й прообразу.

1.1. Визначити: $\overline{T}_V,\overline{\overline{T}}_V$ – внутрішності $\overline{T},\overline{\overline{T}}$ відповідно;

1.2. Визначити: $\overline{B}^{(1)}$ і $\overline{\overline{B}}^{(1)}$; $\overline{B}^{(2)}$ і $\overline{\overline{B}}^{(2)}$; …; $\overline{B}^{(t)}$ і $\overline{\overline{B}}^{(t)}$ – пари відповідних $l\times l$ - блоків ЦЗ таких, що

$$\overline{B}^{(k)}\subseteq\overline{T}_V,\ \ \overline{\overline{B}}^{(k)}\subseteq\overline{\overline{T}}_V,\ k=\overline{1,t}. \qquad (15.1)$$

1.3. Надати: $\overline{p}=0,\ \overline{\overline{p}}=0$ – лічильники, що показують скільки разів у ході роботи методу як клон визначалася область $\overline{T},\overline{\overline{T}}$ відповідно.

Крок 2. Для кожної пари відповідних блоків $\overline{B}^{(k)}, \overline{\overline{B}}^{(k)}$, $k = \overline{1,t}$, виділених попередньо областей клону й прообразу:

2.1. Отримати відповідно $\overline{R}^{(k)}, \overline{\overline{R}}^{(k)}$ – блоки ЦЗ, розташування яких відповідає зсуву $\overline{B}^{(k)}, \overline{\overline{B}}^{(k)}$ на 1 піксель в обраному напрямку v.

2.2. Для блоків $\overline{R}^{(k)}, \overline{\overline{R}}^{(k)}$ побудувати $\overline{O}, \overline{\overline{O}}$ – відповідні відмітні околи радіуса 1.

2.3. Знайти $\left\|\overline{O}\right\|, \left\|\overline{\overline{O}}\right\|$ – матричні норми $\overline{O}, \overline{\overline{O}}$.

2.4. *Якщо*

$$\left\|\overline{O}\right\| = \left\|\overline{\overline{O}}\right\|,$$

то

$\overline{R}^{(k)} \subseteq \overline{P}_V$, $\overline{\overline{R}}^{(k)} \subseteq \overline{\overline{P}}_V$, де $\overline{P}_V$, $\overline{\overline{P}}_V$ – внутрішності $\overline{P}, \overline{\overline{P}}$ відповідно,

границі клону й прообразу не досягнуті,

$\overline{B}^{(k)} = \overline{R}^{(k)}, \overline{\overline{B}}^{(k)} = \overline{\overline{R}}^{(k)}$, перехід на крок 2.1;

інакше

якщо $\left\|\overline{O}\right\| > \left\|\overline{\overline{O}}\right\|,$

то $\overline{p} = \overline{p} + 1,$

інакше $\overline{\overline{p}} = \overline{\overline{p}} + 1.$

2.5. *Якщо* потрібно уточнення отриманих результатів $\overline{p}$, $\overline{\overline{p}}$,

то повернутися до первісних блоків $\overline{B}^{(k)}, \overline{\overline{B}}^{(k)}$, місце розташування яких визначено на кроці 1;

змінити напрямок v їх зсуву. Перехід на крок 2.1.

Крок 3 *(відокремлення клону від прообразу)*.

Якщо $\overline{p} > \overline{\overline{p}}$,

то $\overline{T}$ – клон, $\overline{\overline{T}}$ – прообраз,

інакше $\overline{T}$ – прообраз, $\overline{\overline{T}}$ – клон.

В алгоритмічній реалізації методу: як v завдяки кроку 2.5 використовуються 8 різних напрямків зсуву блоків: додатний, від'ємний напрямки координатних осей, а також напрямки, що відповідають діагоналям (головній й побічній) блоків (вздовж них – вгору, вниз); $t = 1$: у внутрішностях областей $\overline{T}, \overline{\overline{T}}$ клону й прообразу обиралася лише одна пара відповідних блоків: $\overline{B}^{(1)}, \overline{\overline{B}}^{(1)}$; $l \geq 8$. Вибір розміру *l* визначався розмірами областей клону й прообразу.

Для оцінки ефективності запропонованої алгоритмічної реалізації методу *KP2* був проведений обчислювальний експеримент, у якому було задіяні 500 ЦЗ із бази NRCS. Експеримент будувався наступним чином. Оригінальні ЦЗ піддавалися клонуванню (без обмежень на форму областей прообразу/клону, при цьому клон і прообраз були такими, щоб лінійні розміри прямокутників, що в них вписуються, не були менше 8 (обмеження пов'язано з тим, що більшість з існуючих на сьогоднішній день методів й алгоритмів не виявляють систематично області клону й прообразу менших розмірів, крім того, для виявлення моменту

досягнення (переходу) через границю клона/прообраза блоки $\overline{B}^{(1)}, \overline{\overline{B}}^{(1)}$ не можуть мати довільно малі розміри)), після чого зберігалися у форматі без втрат (Tif). Області клону й прообразу $\overline{T}, \overline{\overline{T}}$ вважалися відомими (виявленими деяким відповідним алгоритмом) на кроці 1 алгоритмічної реалізації розробленого методу. Для зменшення обчислювальної складності алгоритму l вибиралося якнайбільше з урахуванням задоволення умов (15.1), що накладаються на блоки $\overline{B}^{(1)}, \overline{\overline{B}}^{(1)}$. Аналіз областей клону/прообразу чергового ЦЗ завершувався, як тільки $\overline{p}$ чи $\overline{\overline{p}}$ досягало значення 5 (з урахуванням використання 8 різних напрямків для v). Результати експерименту, які говорять про високу ефективність методу, представлені в табл. 15.3, де кількість помилок визначалася відносною кількістю ЦЗ (вираженою у відсотках від загальної кількості проаналізованих зображень), де клон і прообраз були відокремлені не вірно.

Таблиця 15.3

Відносна кількість (%) помилок при відокремленні клону від прообразу в умовах відсутності будь-якої постобробки клонованого ЦЗ

l	8	16	24	32
Кількість помилок	6.5	7	5.5	4.5

Питання

1. Два підходи, що застосовуються для відокремлення клону від прообразу. Характеристики, недоліки кожного з них.
2. Локальне порушення цілісності в умовах клонування.
3. Основні проблеми при відокремленні клону від прообразу. Пояснити.
4. Теоретичні основи відокремлення клону від прообразу в цифровому зображенні в умовах відсутності відмінностей в їх постобробці.
5. Основні кроки методу відокремлення клону від прообразу в умовах відсутності постобробки зображення

Література

1. Бобок І.І. Підвищення інформативності результатів виявлення клонування в цифровому зображенні. *Збірник наукових праць ВІКНУ імені Тараса Шевченка*. 2017. 58. С. 81–90.
2. Бобок И.И., Дзюбинская Л.М., Кобозева А.А. Выявление нарушений целостности цифрового изображения путем использования стеганографических алгоритмов. *Інформатика та математичні методи в моделюванні*. 2015. 5(2). С. 129–134.
3. Хорошко В.О., Бобок І.І. Удосконалення методу виявлення результатів клонування в цифровому зображенні. *Вісник ЧДТУ: Технічні науки*. 2019. 3. С. 38–49.
4. Бобок І.І., Кобозєва А.А. Теоретичні основи методу відокремлення клону від прообразу в цифровому зображенні. *Безпека інформації*. 2018. 24(1). С. 49–55.
5. Бобок І.І. Метод відокремлення клону від прообразу в цифровому зображенні в умовах відсутності відмінностей при їх постобробці. *Інформатика та математичні методи в моделюванні*. 2017. 7(4). С. 276–284.
6. Бобок І.І., Кобозєва А.А. Метод відокремлення клону від прообразу в цифровому зображенні в умовах відсутності постобробки зображення. *Вісник ЧДТУ: Технічні науки*. 2018. 2. С. 12–19.
7. Хорошко В.О., Бобок І.І. Виявлення локального порушення цілісності цифрового зображення. *Інформатика та математичні методи в моделюванні*. 2019. 9(1-2). С. 24–37.