Міністерство освіти та науки України

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
«ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ПІДХОДИ ДО ЇХ ВИРІШЕННЯ»

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації

Одеса, 2025

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

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

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

ЗМІСТ

ВСТУП

Дисципліна «Проблеми кібербезпеки та сучасні підходи до їх вирішення» відповідає освітньо-професійній програмі, навчальному плану підготовки фахівців другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації, 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 інформаційної безпеки.

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

Мета лабораторних занять полягає у практичному формуванні та розвитку відповідних професійних компетентностей майбутніх фахівців, які слугуватимуть підґрунтям для їхньої практичної роботи, що пов'язана із забезпеченням захисту інформації та організацією інформаційної та кібербезпеки.

Лабораторна робота №1.

Дослідження чутливості параметрів повного набору матриці інформаційної системи до збурень вхідних даних

Мета роботи: Планування та виконання експериментальних досліджень для практичної перевірки нечутливості сингулярних чисел (власних значень) матриці (зображення, кадра відео) до збурних дій, наявності в межах одної матриці сингулярних векторів (власних векторів) як чутливих, так і нечутливих до збурних дій, дослідження ступеня чутливості сингулярних векторів.

Лабораторна робота №1 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

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

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

1.1. 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 приклад.

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 (або погано обумовленою, або некоректно поставленою).

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:

$$\overline{\lim_{\overline{\xi} \to \xi}} \frac{\textit{відстань між } \phi(\xi) \textit{ і } \phi(\overline{\xi})}{\textit{відстань між } \xi \textit{ і } \overline{\xi}}. \qquad (1.1)$$

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. Для кожної конкретної задачі цей вираз буде мати свій конкретний вигляд, наприклад, для задачі розвязку системи лінійних алгебраїчних рівнянь з матрицею A, число обумовленості буде дорінювати $\|A\| \cdot \|A^{-1}\|$, де $\|\bullet\|$ - матрична норма, A^{-1} - матриця, обернена до A.

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.

1.2. Формальне представлення інформаційної системи та її перетворення

У якості математичної моделі будь-якої інофрмаційної системи (ІС) будемо розглядати одну двовимірну (прямокутну або квадратну) матрицю F.

Результат будь-яких дій над ІС, що моделюється, у загальному випадку можна представити як збурення ΔF матриці 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:

$$\overline{F} = F + \Delta F,$$

де $\Delta F = f(F)$ - матриця того ж розміру, що і F, яка є деякою функцією матриці F.

Таким чином, ***будь-які перетворення довільної ІС можуть бути формально представлені у вигляді елементарних матричних операцій***

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*.

Один з таких наборів представляе з себе множину сингулярних чисел і лівих і правих сингулярних векторів, які однозначно визначаються за допомогою нормального сингулярного розкладання.

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 сингулярне розкладання (SVD - *Singular value decomposition*):

$$F = U \Sigma V^T, \qquad (1.2)$$

де U, V — матриці розміром $m \times n$ і $n \times n$ відповідно;

$\Sigma = diag(\sigma_1,...,\sigma_n)$,

$$\sigma_1 \geq ... \geq \sigma_n \geq 0. \qquad (1.3)$$

При цьому U, V задовольняють співвідношенням: $U^TU = I$, $V^TV = I$, де I — одинична матриця відповідного розміру, тобто є ортогональними. Стовпці $u_1,...,u_n$ матриці U і $v_1,...,v_n$ матриці V - *ліві і праві сингулярні вектори* матриці F, величини $\sigma_1,...,\sigma_n$ — *сингулярні числа* (СНЧ).

У загальному випадку SVD матриці визначається неоднозначно. Вектор u називається *лексикографічно додатним*, якщо його перший ненульовий компонент додатний, а SVD (1.2) *нормальним*, якщо стовпці матриці U лексикографічно додатні. Можна показати, що невироджена матриця має єдине нормальне SVD, якщо її СНЧ попарно різні.

Отримати сингулярне розкладання матриці F в середовищі *Matlab* можливо за допомогою вбудованої функції *svd*:

```
>> [U,SIGMA,V]=svd(F);
```

Результат розкладання – матриці U, V (лівих і правих векторів відповідно), діагональна матриця SIGMA (на діагоналі – СНЧ). В загальному випадку отримуване тут розкладання не є нормальним, тому не є таким, що визначається однозначно. Так для 8*8-матриці

$$M = \begin{pmatrix} 162 & 144 & 128 & 124 & 128 & 132 & 136 & 136 \\ 146 & 129 & 118 & 112 & 113 & 117 & 119 & 118 \\ 129 & 134 & 138 & 141 & 142 & 140 & 140 & 144 \\ 156 & 161 & 163 & 163 & 162 & 165 & 167 & 169 \\ 179 & 180 & 179 & 177 & 175 & 175 & 174 & 174 \\ 178 & 176 & 177 & 177 & 174 & 173 & 171 & 165 \\ 177 & 176 & 177 & 177 & 176 & 175 & 170 & 159 \\ 175 & 175 & 174 & 173 & 170 & 165 & 161 & 156 \end{pmatrix} \qquad (1.4)$$

в результаті сингулярного розкладання отримано:

$$U = \begin{pmatrix} -0.3056 & -0.6215 & 0.3218 & -0.1994 & -0.3132 & 0.3921 & 0.3260 & -0.1379 \\ -0.2726 & -0.5784 & 0.0799 & 0.1066 & 0.2102 & -0.5100 & -0.4407 & 0.2738 \\ -0.3101 & 0.3945 & 0.3898 & -0.0379 & -0.6737 & -0.2713 & -0.2586 & 0.0214 \\ -0.3656 & 0.3140 & 0.5018 & -0.0211 & 0.5078 & 0.1812 & 0.1995 & 0.4300 \\ -0.3958 & 0.0837 & 0.0428 & 0.4360 & 0.2383 & 0.2319 & -0.3158 & -0.6589 \\ -0.3897 & 0.0811 & -0.2173 & -0.1140 & 0.1006 & -0.5736 & 0.5955 & -0.2960 \\ -0.3886 & 0.1062 & -0.4261 & -0.6948 & 0.0779 & 0.2202 & -0.3435 & 0.0298 \\ -0.3780 & 0.0116 & -0.5057 & 0.5111 & -0.2701 & 0.2202 & 0.1434 & 0.4450 \end{pmatrix}$$

```
V =
   -0.3656   -0.8207   -0.1041   -0.1141   -0.1721   -0.3719   -0.0162   -0.0270
   -0.3597   -0.2491   -0.1767    0.3459    0.1407    0.7824    0.1317   -0.0914
   -0.3550    0.1872   -0.3247    0.3568    0.4630   -0.3081   -0.3848    0.3857
   -0.3525    0.3504   -0.3319    0.1398   -0.1227   -0.3113    0.5544   -0.4515
   -0.3509    0.2675   -0.1791   -0.1965   -0.7174    0.1772   -0.1920    0.3895
   -0.3510    0.1528    0.0443   -0.5376    0.2337    0.1109   -0.4703   -0.5238
   -0.3493    0.0628    0.3283   -0.4411    0.3476    0.0333    0.5029    0.4436
   -0.3439    0.0879    0.7749    0.4452   -0.1760   -0.1135   -0.1265   -0.1242
```

```
SIGMA =
1.0e+003 *
    1.2622         0         0         0         0         0         0         0
         0    0.0426         0         0         0         0         0         0
         0         0    0.0246         0         0         0         0         0
         0         0         0    0.0062         0         0         0         0
         0         0         0         0    0.0038         0         0         0
         0         0         0         0         0    0.0020         0         0
         0         0         0         0         0         0    0.0011         0
         0         0         0         0         0         0         0    0.0002
```

Очевидно, що це розкладання не є нормальним, оскільки не всі стовпці матриці *U* є лексикографічно додатними: 1-й, 2-й, 4-й, 5-й, 8-й мають перші ненульові елементи від'ємними. Для забезпечення єдиності розкладання треба забезпечити його нормальність, перевіряючи кожен стовпець *U* на лексикографічну додатність:

```
>> %  цикл по всіх стовпцях матриці U
>> for i=1:1:8
      if U(1,i)<0
         U(:,i)=-U(:,i);
   %  зміна відбувається і з відповідним правим СНВ, тобто і-им стовпцем
   %  матриці V
         V(:,i)=-V(:,i);
      end
   end
```

В результаті отримані:

```
U =
   0.3056    0.6215    0.3218    0.1994    0.3132    0.3921    0.3260    0.1379
   0.2726    0.5784    0.0799   -0.1066   -0.2102   -0.5100   -0.4407   -0.2738
   0.3101   -0.3945    0.3898    0.0379    0.6737   -0.2713   -0.2586   -0.0214
   0.3656   -0.3140    0.5018    0.0211   -0.5078    0.1812    0.1995   -0.4300
   0.3958   -0.0837    0.0428   -0.4360   -0.2383    0.2319   -0.3158    0.6589
   0.3897   -0.0811   -0.2173    0.1140   -0.1006   -0.5736    0.5955    0.2960
   0.3886   -0.1062   -0.4261    0.6948   -0.0779    0.2202   -0.3435   -0.0298
   0.3780   -0.0116   -0.5057   -0.5111    0.2701    0.2202    0.1434   -0.4450
```

$$V = \begin{pmatrix} 0.3656 & 0.8207 & -0.1041 & 0.1141 & 0.1721 & -0.3719 & -0.0162 & 0.0270 \\ 0.3597 & 0.2491 & -0.1767 & -0.3459 & -0.1407 & 0.7824 & 0.1317 & 0.0914 \\ 0.3550 & -0.1872 & -0.3247 & -0.3568 & -0.4630 & -0.3081 & -0.3848 & -0.3857 \\ 0.3525 & -0.3504 & -0.3319 & -0.1398 & 0.1227 & -0.3113 & 0.5544 & 0.4515 \\ 0.3509 & -0.2675 & -0.1791 & 0.1965 & 0.7174 & 0.1772 & -0.1920 & -0.3895 \\ 0.3510 & -0.1528 & 0.0443 & 0.5376 & -0.2337 & 0.1109 & -0.4703 & 0.5238 \\ 0.3493 & -0.0628 & 0.3283 & 0.4411 & -0.3476 & 0.0333 & 0.5029 & -0.4436 \\ 0.3439 & -0.0879 & 0.7749 & -0.4452 & 0.1760 & -0.1135 & -0.1265 & 0.1242 \end{pmatrix}$$

Очевидно, що таке сингулярне розкладання є нормальним.

Будь-яке перетворення ІС збурить її матрицю F, а тому певним чином збурить її СНЧ і СНВ. Тому ***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.

1.3. Чутливість сингулярних чисел матриці до збурних дій

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

$$\max_{1\le j\le N}\left|\sigma_j(F)-\sigma_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2, \qquad (1.5)$$

де $\left\|\bullet\right\|_2$ — спектральна матрична норма (СМН), тобто при збуренні матриці F (вхідних даних) СНЧ зазнають адекватних змін, вони є добре обумовленими, чи нечутливими до змін вхідних даних.

Приклад. Розглянемо (в середовищі *Matlab*) оригінальне цифрове зображення (ЦЗ) (рис.1.1(а)) розміром 400*400 пікселів (кольорова схема RGB), що зчитується в змінну *A*:

```
>> A=imread('F:\4cam_auth\4cam_auth\036.tif');
```

яке піддамо незначній, що є природнім на практиці, збурній дії: накладанню гауссівського шуму з нульовим математичним очікуванням і дисперсією 0.0001:

```
>> A1=imnoise(A,'gaussian',0,0.0001);
```

(рис.1.1(б)). З кожного з зображень виділимо одну кольорову складову, наприклад, синю, яку відповідно позначимо *F* і *F1*:

```
>> F=A(:,:,3); F1=A1(:,:,3);
```

Для 400*400-матриці збурення $\Delta F = F1 - F$ матрична норма, яка є кількісним показником збурення вхідних даних, дорівнює $\|\Delta F\| = 100.9409$.

а

б

Рис.1.1. ЦЗ, що розглядається в прикладі: а – оригінальне ЦЗ; б – збурене ЦЗ

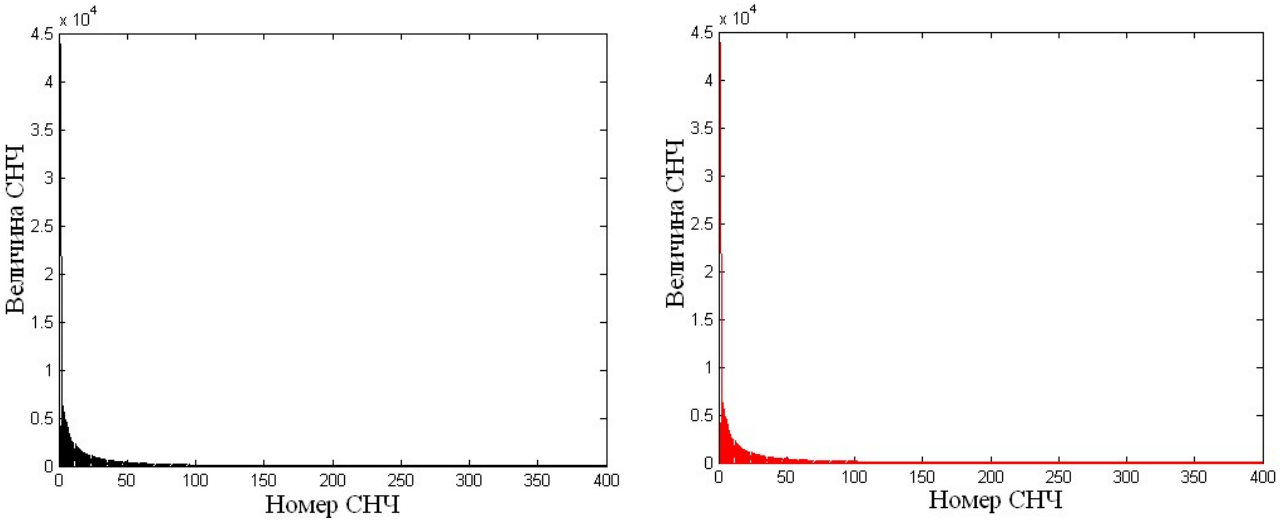
Шляхом побудови сингулярного розкладання обчислимо СНЧ F і $F1$, які будуть збережені в діагональних матрицях SIGMA і SIGMA1 відповідно:

```
>> [U,SIGMA,V]=svd(F);
>> [U1,SIGMA1,V1]=svd(F1);
```

Графіки залежності значення СНЧ від його номеру для F і $F1$, отримані в середовищі *Matlab* за допомогою:

```
>> i=1:1:400;
>> plot(i,SIGMA(i,i),'k-');
>> figure;
>> plot(i,SIGMA1(i,i),'r-');
```

представлені на рис.1.2. Завдяки значному розкиду значень СНЧ для ЦЗ на отриманих графіках дуже складно відстежити збурення СНЧ, що чітко видно на рис.1.3, який наочно ілюструє нечутливість СНЧ до збурних дій: значення збурень СНЧ не перевищують збурення вхідних даних $\|\Delta F\| = 100.9409$.



а б

Рис.1.2. Графіки залежности величини СНЧ від його номеру для: а – оригінального ЦЗ; б – збуреного ЦЗ

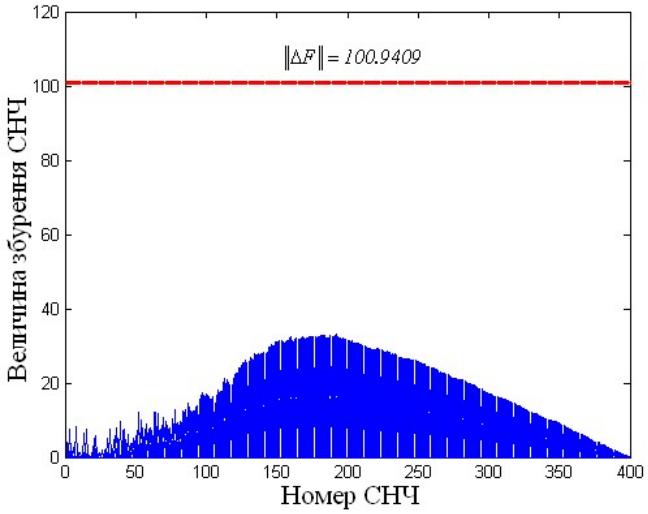


Рис.1.3. Графік залежності збурення СНЧ від його номеру

1.4. Відокремленість сингулярного числа матриці

Відокремленістю СНЧ σ_i матриці F називається величина:

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

На практиці для обчислення відокремленості σ_i треба обрати найменшу з відстаней від σ_i до найближчих до нього СНЧ: σ_{i-1}, σ_{i+1}. Для першого СНЧ очевидно, що

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

а для останнього – це буде модуль різниці двох останніх СНЧ.

Відокремленість СНЧ відіграє дуже важливу роль для чутливлості відповідного СНВ матриці.

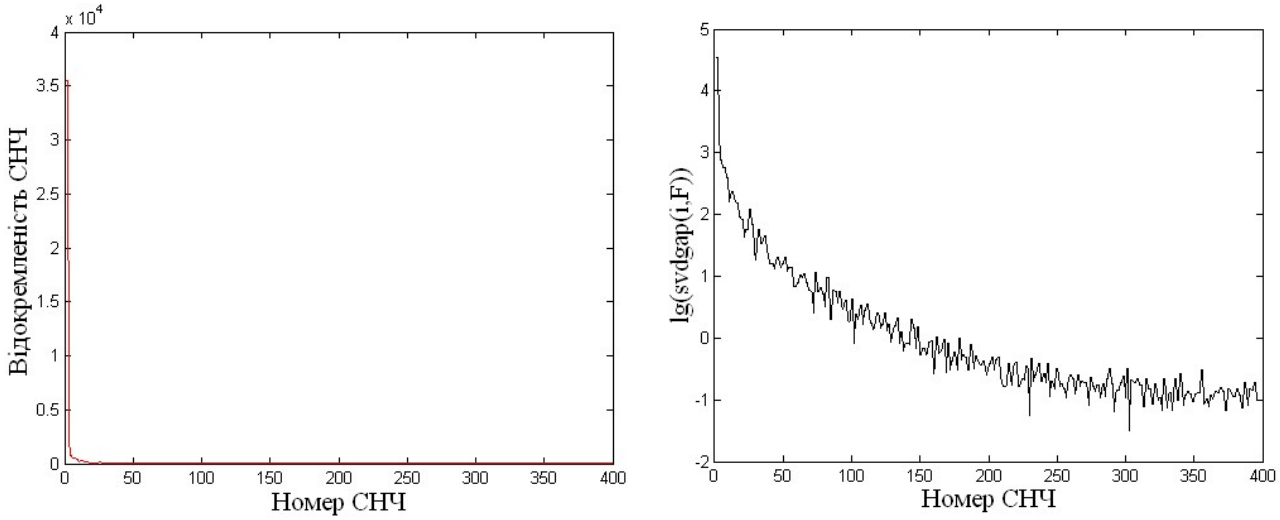
Для СНЧ матриць оригінальних ЦЗ, кадрів цифрового відео співвідношення (1.3) можна уточнити:

$$\sigma_1 >> \sigma_2 \geq \ldots \geq \sigma_n \geq 0, \qquad (1.6)$$

що дуже яскраво видно на рис.1.2. Це приводе до того, що відокремленість першого СНЧ є набагато більшою за відокремленості всіх інших СНЧ. Для ілюстрації цього факту розглянемо зображення на рис.1.1(а) (синю кольорну складову). Для обчислення відокремленостей СНЧ матриці синьої складової ЦЗ в середовищі *Matlab* можливо зробити наступне (відокремленості зберігаються в масиві SVDGAP):

```
>> N=400;
>> for i=2:1:(N-1)
     SVDGAP1=SIGMA(i-1,i-1)-SIGMA(i,i); % відстань між і-м та (і-1)-м  СНЧ
     SVDGAP2=SIGMA(i,i)-SIGMA(i+1,i+1); % відстань між і-м та (і+1)-м  СНЧ
     SVDGAP(i)=min(SVDGAP1,SVDGAP2);
   end
>> SVDGAP(1)=SIGMA(1,1)-SIGMA(2,2);
>> SVDGAP(N)=SIGMA(N-1,N-1)-SIGMA(N,N);
```

Графік залежності відокремленості СНЧ від його номеру представлений на рис.1.4 (а). Для більш наочної якісної картини на рис.1.4(б) побудований графік залежності десяткового логарифма відокремленості СНЧ від його номеру.



а б

Рис.1.4. Ілюстрація зміни відокремленості СНЧ зі зростанням його номеру: а - графік залежності відокремленості СНЧ від його номеру; б - графік залежності десяткового логарифма відокремленості СНЧ від його номеру

1.5. Чутливість сингулярних векторів матриці до збурних дій

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

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F)} \text{ за умови } svdgap(i,F) \neq 0, \qquad (1.7)$$

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F+\Delta F)} \text{ за умови } svdgap(i,F+\Delta F) \neq 0. \qquad (1.8)$$

Таким чином, виходячи з (1.7), (1.8), 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, тим меншою буде його зміна, реакція на цю збурну дію.

Для ілюстрації цього повернемося до матриці M (1.4) оригінального ЦЗ, для якої в розділі 1.2 були отримані СНЧ і СНВ. З матриці M за допомогою матриці ΔM

$$\Delta M = \begin{pmatrix} -1 & 2 & 1 & 0 & 2 & 2 & -2 & 0 \\ 0 & 0 & -2 & 2 & 3 & 3 & 0 & 0 \\ -3 & 1 & 1 & 0 & 3 & -3 & 1 & 4 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 2 & -5 & 2 & 3 & 3 \\ 0 & 2 & 1 & 0 & 4 & 0 & -1 & 0 \\ 0 & 1 & 0 & -5 & 0 & -5 & 0 & 0 \\ -4 & 0 & 2 & 0 & 5 & 0 & 1 & -6 \end{pmatrix}$$

отримаємо збурену матрицю M1. Для обох матриць M, M1 знайдемо СНВ за допомогою нормального сингулярного розкладання. Для кожного СНВ U(:,i) матриці M визначимо його збурення в результаті збурної дії ΔM, порівнявши з відповідним СНВ $U1$(:,i) матриці M1 шляхом обчислення норми вектора різниці $\|U(:,i)-U1(:,i)\|$ і зберігаючи в DELTAU:

```
>>for i=1:1:N
      DELTAU(i)=norm(U(:,i)-U1(:,i));
  end
```

Результати наведені на рис.1.5, звідки очевидна відповідність оцінки чутливості СНВ формулам (1.7), (1.8), зокрема обернена залежність кількісної оцінки чутливості від відокремленості СНЧ. Очевидно, що нечутливими до збурних дій будуть СНВ, що відповідають максимальним СНЧ ЦЗ. При порівнянні графіків, представлених на рис.1.5(а), 1.5(б) наочно видно, що збурна дія завдякі нечутливості СНЧ, незначно змінює їх відокремленості, що

дійсно дозволяє оцінювати чутливість СНВ як за формулою (1.7), так і за формулою (1.8), що є дуже важливим тоді, коли оригінального цифрового контента в наявності немає. Всі ці властивості будуть зберігатися для будь-якої підматриці матриці поданого цифрового контенту.

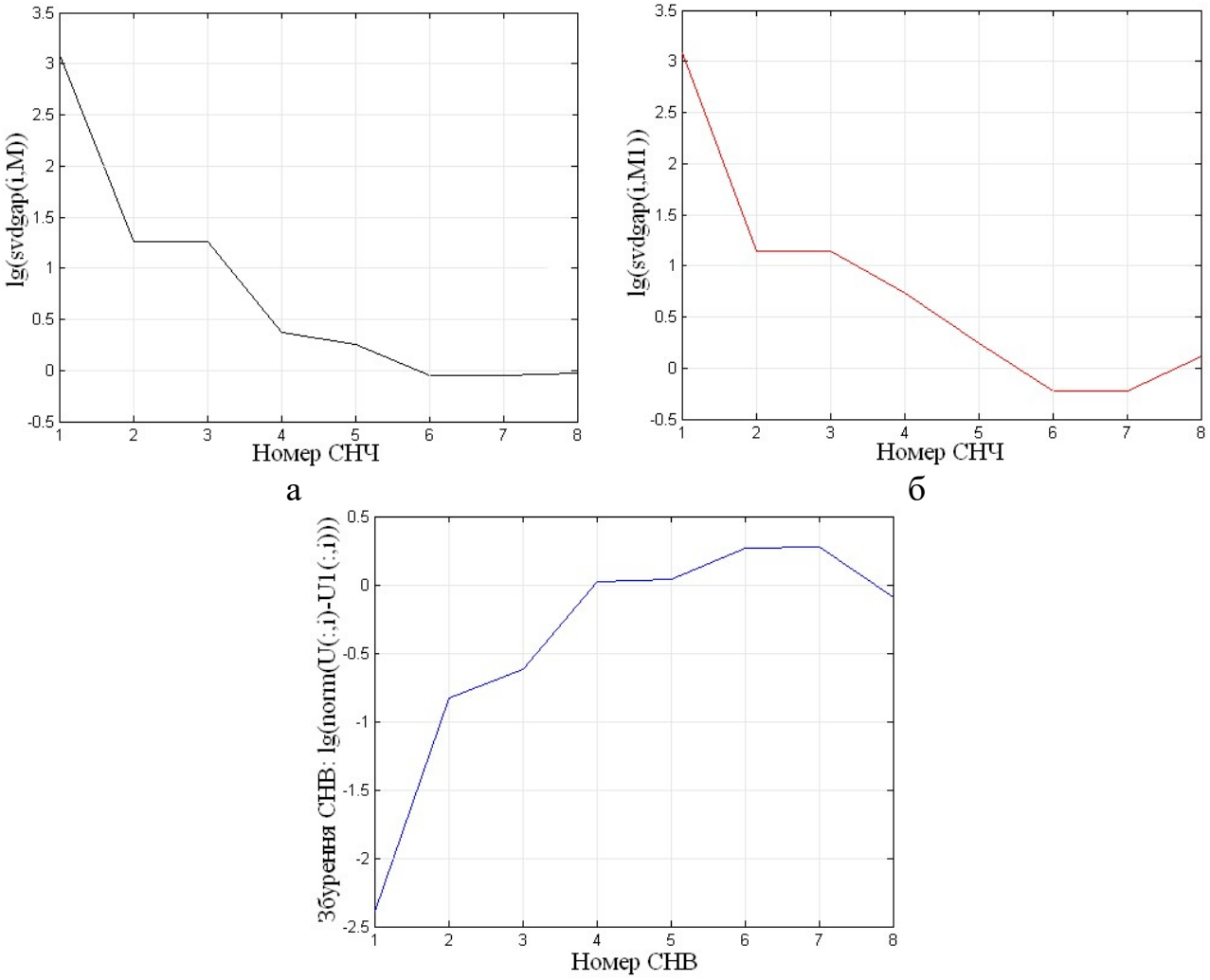


Рис.1.5. Ілюстрація залежності збурення СНВ від відокремленості відповідного СНЧ: а – графік залежності відокремленості СНЧ матриці М від його номеру; б - графік залежності відокремленості СНЧ збуреної матриці М1 від його номеру; в – графік залежності збурення лівого СНВ від його номеру

Визначення 1.1. *Чутливістю* ІС назвемо чутливість задачі її формування.

У силу співвідношення (1.5) 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.

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

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

1.6. Повний набір формальних параметрів симетричної матриці

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:

$$F=U\Lambda U^T \tag{1.9}$$

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

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, що приводить до неоднозначного визначення спектрального розкладання (1.9).

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

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

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 (1.5):

$$\max_{1\leq j\leq n}\left|\lambda_j(F)-\lambda_j(F+\Delta F)\right|\leq\left\|\Delta F\right\|_2, \tag{1.10}$$

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:

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

$$sin\,\theta_i\leq\frac{2\left\|\Delta F\right\|_2}{gap_{abs}(i,\overline{F})}\ , \tag{1.12}$$

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

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

$$gap_{abs}(i, \mathrm{F}) = \min_{i \neq j} \left\| \lambda_j \right| - \left| \lambda_i \right\|$$

— абсолютна відокремленість ВЗ λ_i матриці F.

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

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

1.7. Зведення формального представлення інформаційної системи до симетричної матриці

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, 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:

$$F = \begin{pmatrix} a_{11}\, a_{12}\ a_{13} \ldots a_{1n} \\ a_{21}\, a_{22}\ a_{23} \ldots a_{2n} \\ a_{31}\, a_{32}\ a_{33} \ldots a_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}\, a_{n2}\ a_{n3} \ldots a_{nn} \end{pmatrix} \rightarrow A = \begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{1n} \\ a_{12}\, a_{22}\, a_{23} \ldots a_{2n} \\ a_{13}\, a_{23}\, a_{33} \ldots a_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}\, a_{2n}\, a_{3n} \ldots a_{nn} \end{pmatrix}, B = \begin{pmatrix} a_{11}\, a_{21}\, a_{31} \ldots a_{n1} \\ a_{21}\, a_{22}\, a_{32} \ldots a_{n2} \\ a_{31}\, a_{32}\, a_{33} \ldots a_{n3} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}\, a_{n2}\, a_{n3} \ldots a_{nn} \end{pmatrix}, \quad (1.13)$$

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 (1.13), 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 $\overline{B}$.

Такий підхід дає можливість розглядати в якості формального представлення будь-якої інформаційної системи симетричну матрицю (матриці).

Завдання до лабораторної роботи №1

1. Зчитати кольорове цифрове зображення (схема RGB), яке може бути сформоване непрофесійною відеокамерою або взяте з одної з традиційних баз, що використовуються під час роботи з зображеннями, наприклад, бази NRCS https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
2. Виділити з зображення одну кольорову складову K, яку обрізати до розміру N*N. Нехай N*N-матриця A є результатом.
3. Для матриці A за допомогою сингулярного чи спектрального розкладання (після попереднього потрібного перетворення матриці, яке приведе її до симетричного виду), яке зробити шляхом використання вбудованих в *Matlab* функцій *svd* (сингулярне розкладання) або *eig* (спектральне розкладання), отримати набори N сингулярних чисел (N власних значень), по N лівих і правих сингулярних векторів (N власних векторів).
4. Піддати цифрове зображення збурній дії D.
5. Провести кроки 2 (матриця, отримувана на кроці 2, A_D), 3 для спотвореного зображення.
6. Перевірити, що сингулярні числа (власні значення) є нечутливими до збурної дії (див.(1.5)). Побудувати (в середовищі *Matlab*) графік залежності збурення сингулярного числа (власного значення) від його номеру. Пояснити.
7. Виділити сингулярні вектори, що є очікувано найменш і найбільш чутливими до збурної дії, скориставшись формальним показником нечутловисті для цих векторів (відокремленістю відповідного сингулярного числа чи абсолютною відокремленістю відповідного власного значення (див. (1.7), (1.8)).
8. Виділити сингулярні вектори, що є на практиці найменш і найбільш чутливими до збурної дії, шляхом безпосереднього обчислення збурення для кожного сингулярного вектора (власного вектора). Це можна зробити: за допомогою обчислення кута повороту кожного вектора в результаті збурної дії; за допомогою обчислення норми вектора різниці відповідних сингулярних векторів (власних векторів) до і після збурної дії.
9. Дослідити відповідність/невідповідність ступеня чутливості до збурної дії сингулярних векторів (власних векторів), отриманої теоретично та практично. При виникненні невідповідності, пояснити отримані результати.
10. Побудувати (в середовищі *Matlab*) графіки залежності збурення сингулярних векторів (власного значення), обчисленого на кроці 8, від їх номера;

відокремленості (абсолютної відокремленості) сингулярного числа (власного значення) від його номера; залежності збурення сингулярних векторів (власного значення), обчисленого на кроці 8, від відокремленості (абсолютної відокремленості) сингулярного числа (власного значення). Пояснити отримані залежності. Чи відповідають вони теоретичним очікуванням? Якщо ні, то чому?

11. Незначно змінити заданий параметр збурної дії. Проробити кроки 2-10 в умовах нової збурної дії. Порівняти отримані відповідні графіки для різних збурних дій. Дослідити та пояснити якісні і кількісні збіжності і розбіжності в графіках.
12. Повторити кроки 1-11 для 100 ЦЗ. Зробити загальні висновки відносно чутливості складових повного набору формальних параметрів матриці.
13. Зробити порівняльний аналіз результатів, отриманих варінтами завдань 1 і 3, 2 і 4, 5 і 7, 6 і 8, 9 і 10.

Варіанти завдання

1. K=G; N=400; використовується сингулярне розкладання матриці; D – гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.0001.
2. K=B; N=400; використовується сингулярне розкладання матриці; D – мультиплікативний шум з дисперсією d=0.0001.
3. K=G; N=400; використовується спектральне розкладання матриці; D – гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.0001.
4. K=B; N=400; використовується спектральне розкладання матриці; D – мультиплікативний шум з дисперсією d=0.0001.
5. K=R; N=300; використовується сингулярне розкладання матриці; D – пуассонівський шум.
6. K=G; N=300; використовується сингулярне розкладання матриці; D – мультиплікативний шум з дисперсією d=0.00001.
7. K=R; N=300; використовується спектральне розкладання матриці; D – пуассонівський шум.
8. K=G; N=300; використовується спектральне розкладання матриці; D – мультиплікативний шум з дисперсією d=0.00001.
9. K=G; N=500; використовується сингулярне розкладання матриці; D відповідає матриці збурення, яку сформувати самостійно.
10. K=B; N=300; використовується сингулярне розкладання матриці; D відповідає матриці збурення, яку сформувати самостійно.
11. K=G; N=500; використовується спектральне розкладання матриці; D відповідає матриці збурення, яку сформувати самостійно.
12. K=B; N=300; використовується спектральне розкладання матриці; D відповідає матриці збурення, яку сформувати самостійно.

Контрольні запитання

1. Чому характерні властивості СНЧ (ВЗ) і СНВ (ВВ) матриці є важливими в області інформаційної безпеки?
2. Чи можна робити аналіз чутливості параметрів цифрового зображення поблоково, розглядаючи його як сукупність блоків, отриманих шляхом стандартної розбивки? Якщо так, то в чому полягають переваги та недоліки такого способу?
3. Що можна сказати про обчислювальну складність будь-якого алгоритму, що робить блокову обробку матриці (зображення)?
4. Для оцінки ступеня чутливості сингулярних векторів (власних векторів) матриці до збурних дій можна користуватися як формулою (1.7), так і формулою (1.8) (як формулою (1.11), так і формулою (1.12)). Як це можна пояснити, адже формули різні, а оцінка проводиться одної й тої самої властивості СНВ (ВВ)? Якою саме формулою і в яких саме умовах будете користуватися Ви для оцінки чутливості до збурних дій СНВ (ВВ)? Обгрунтуйте свій вибір.
5. Як Ви вважаєте, які «неприємності» можуть виникнути при користуванні формулами (1.7), (1.8), (1.11), (1.12) в умовах значної збурної дії, в умовах відокремленості СНЧ (ВЗ), порівняної з нульом?
6. Чи відіб'ється на оцінках чутливості СНЧ (ВЗ), СНВ (ВВ) величина розміру матриці? Якщо так, то поясніть, яким саме чином, якщо ні, то поясніть, чому.
7. Чи залежать отримані оцінки чутливостей параметрів, що складають повні набори, від конкретики кольрової складової цифрового зображення? Відповідь поясніть.
8. Чи може СНВ з конкретним номером для одної кольрової складової ЦЗ бути чутливим до збурних дій, а для іншої кольорової складової того ж самого зображення бути нечутливим? Відповідь обгрунтувати.

Лабораторна робота №2

Дослідження надійності сприйняття стеганоповідомлення

Мета роботи: Застосування загального підходу до аналізу інформаційних систем для встановлення ступеня забезпечення надійності сприйняття стеганоповідомлення, отримуваного різними стеганографічними методами. Дослідження відповідності збурень параметрів повного набору контейнера результатам суб'єктивного ранжування та кількісним оцінкам, зробленим за допомогою різницевих показників (PSNR, SNR, MSE). Обгрунтування та розробка пропозицій на основі загального підходу до аналізу інформаційних систем до можливого удосконалення (за необхідності) існуючих стеганоалгоритмів з метою покращення надійності сприйняття відповідних стеганоповідомлень.

Лабораторна робота №2 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

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

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

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

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

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: $\overline{F} = F + \Delta F$. Довільне СПр можна представити у вигляді адитивної вбудови деякої інформації в просторовій області.

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.

СПр представляється у вигляді збурення спектра й (або) ВВ матриці ОП, що визначаються нормальним спектральним розкладанням, у випадку симетричної матриці контейнера.

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, інакше такий прихований канал зв'язку буде розкритий.

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; при $\|\Delta F\| \to 0$ імовірність забезпечення надійності сприйняття буде прямувати до одиниці для кожного ОП. Чим менше $\|\Delta F\|_F$, тим більше ймовірність забезпечення надійності сприйняття для зображення з матрицею $F + \Delta F$ при заданому зображенні F. Ілюстрація наведена на рис.2.1 для оригінального ЦЗ (рис.2.1(а)) розміром 666×1002 пікселя, норма червоної кольорної складової якого становить 3.1830e+007. Норма матриці збурення становила 2.1467e+005 (рис.2.1(б)), 2.1344e+006 (рис.2.1(в)), 6.3776e+006 (рис.2.1(г)).

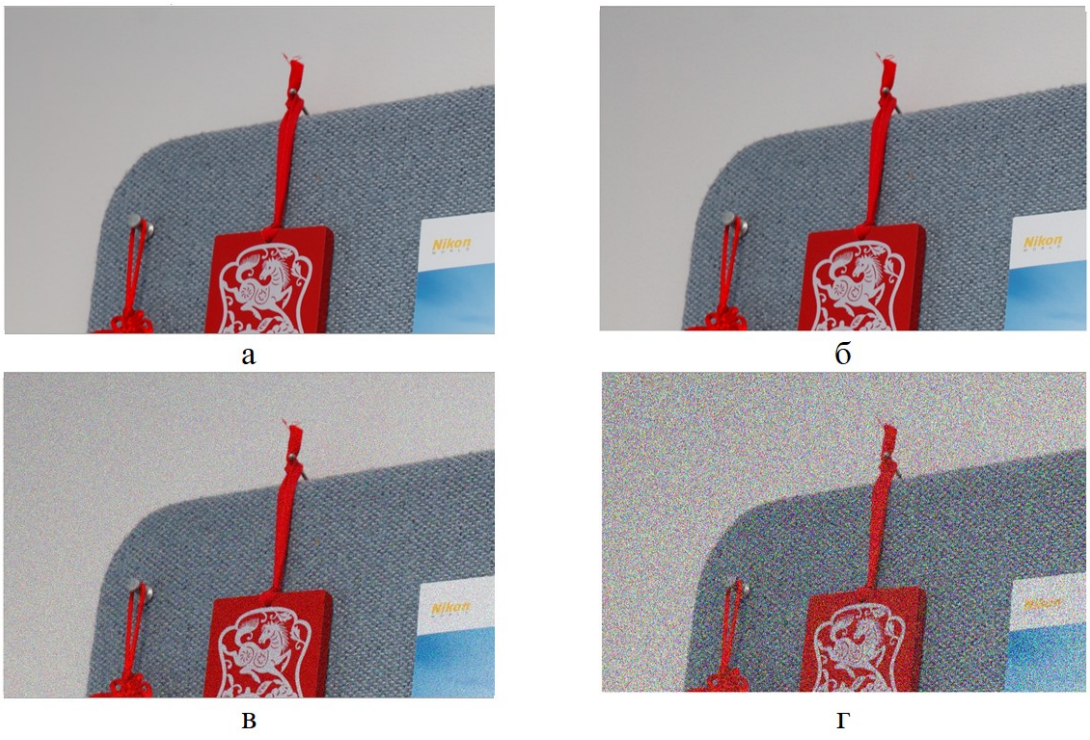


Рис.2.1. Ілюстрація залежності надійності сприйняття ЦЗ від норми матриці збурення

Шляхом субєктивного ранжирування встановлено, що надійність сприйняття для ЦЗ (рис.2.1(б)) не порушена, чого не можна сказати про два інші збурені ЦЗ (рис.2.1(в,г)).

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

Розглядається ОП з довільною матрицею F.

1. Нехай вбудова ДІ викликає збурення $\delta_{k_1},...,\delta_{k_p}$ СНЧ $\sigma_{k_1},...,\sigma_{k_p}$ матриці F ОП. Тоді величина норми матриці збурення ΔF не залежить від того, які саме СНЧ були збурені, а залежить лише від абсолютних величин цих збурень. Ілюстрація наведена на рис.2.2, де незначні збурення (від -2 до +2) зазнали всі СНЧ матриці ЦЗ, що ніяк не порушило надійність сприйняття ЦЗ.

2. Нехай СПр викликало збурення СНВ матриці F ОП. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених СНВ малим по значенню СНЧ F.

3. Нехай СПр збурило СНВ матриці F ОП. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених СНВ сингулярним числам матриці ОП із малою відокремленістю.

При невиконанні умов 2-3 для збурених стеганоперетворенням СНВ великою є ймовірність порушення надійності сприйняття збуреного ЦЗ (рис.2.3 – збурення зазнали СНВ блоків матриці ЦЗ, отриманих шляхом стандартної розбивки, що відповідають максимальним СНЧ блоків (з максимальними відокремленостями)).

а б

Рис.2.2. Ілюстрація збереження надійності сприйняття ЦЗ при незначних збуреннях СНЧ: а – оригінальне ЦЗ; б – збурене ЦЗ

а б

Рис.2.3. Ілюстрація порушення надійності сприйняття ЦЗ при збуренні: а – оригінальне ЦЗ; б – збурене ЦЗ

Таким чином, з метою забезпечення великої ймовірності надійності сприйняття СП вбудову ДІ в контейнер доцільно робити таким чином, щоб збурені стеганоперетворенням СНВ відповідали малим по значенню СНЧ або СНЧ, що мають малі відокремленості, збурення СНЧ були малі.

2.3. Різницеві показники візуального спотворення цифрового зображеня

Нехай F - $n \times m$- матриця ЦЗ-контейнера, а $\overline{F}$ - матриця відповідного стеганоповідомлення. Для обчислення кількісного показника спотворення ЦЗ-контера завдяки стеганоперетворенню можливо використовувати наступні різницеві показники:

- Середньоквадратична похибка (*Mean Square Error*):

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j) - \overline{F}(i,j)\right)^2}{nm};$$

- Нормована середньоквадратична похибка (*Normalized Mean Square Error*):

$$NMSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j) - \overline{F}(i,j)\right)^2}{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j)\right)^2};$$

- Відношення «сигнал-шум» (*Signal to Noise Ratio*):

$$SNR = 10lg\left(\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j)\right)^2}{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j)-\overline{F}(i,j)\right)^2}\right),$$

- Максимальне відношення «сигнал-шум» (*Peak Signal to Noise Ratio*):

$$PSNR = 10lg\left(\frac{M^2}{MSE}\right),$$

де M - максимальне відхилення типу даних вхідного зображення. Наприклад, якщо вхідне зображення має 8-бітовий цілочислений тип даних без знака, M дорівнює 255.

- Якість зображення (*Image Fidelity*):

$$IF = 1 - \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j)-\overline{F}(i,j)\right)^2}{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(F(i,j)\right)^2}.$$

Завдання до лабораторної роботи №2

1. Побудувати програмну реалізацію вбудови додаткової інформації в ЦЗ-контейнер шляхом застосування заданого стеганоалгоритму *S*.
2. Для дослідження залежності/незалежності збереження надійності сприйняття алгоритмом *S*, що розглядається, від формату та якості контейнера сформувати експериментальні множини оригінальних ЦЗ потужністю не менше 100:
    - М1 – ЦЗ у форматі з втратами, обрані з бази зображень;
    - М2 – ЦЗ у форматі без втрат, обрані з бази зображень;
    - М3 – ЦЗ, отримані непрофесійними відеокамерами.
2. Для кожної множини *M1, M2, M3* побудувати відповідні множини стеганоповідомлень $M1_S, M2_S, M3_S$ за допомогою вбудови додаткової інформації стеганоалгоритмом *S*.
3. Для кожної множини встановити порушення/збереження надійності сприйняття стеганоповідомлення за допомогою суб'єктивного ранжирування.
4. Для кожної пари відповідних зображень з множин М1 і $M1_S$, М2 і $M2_S$, М3 і $M3_S$ визначити кількісну оцінку спотворення ЦЗ-контейнера в результаті стеганоперетворення за допомогою різницевого показника *R*. Дослідити, чи

залежить ця оцінка від формату ЦЗ, від якості ЦЗ (ЦЗ, отримані професійними і непрофесійними відеокамерами).

5. Дослідити відповідність між кількісною оцінкою спотворення зображення-контейнера в результаті стеганоперетворення, отриманою за допомогою різницевого показника *R*, і оцінкою, отриманою за допомогою суб'єктивного ранжирування. В результаті встановити значення різницевого показника *R*, яке можна вважати пороговим для висновку про збереження надійності сприйняття стеганоповідомлення алгоритмом *S*.
6. Дослідити, чи задовольняє алгоритм *S* формальній достатній умові збереження надійності сприйняття стеганоповідомлення, заснованій на аналізі СНЧ і СНВ, для чого:
   6.1. Для кожного конкретного ЦЗ:
   - Розбити матриці контейнера та стеганоповідомлення на непересічні $l \times l$ – блоки за допомогою стандартної розбивки;
   - Побудувати сингулярні розкладання відповідних $l \times l$ – блоків матриць контейнера та стеганоповідомлення (якщо алгоритм *S* є блоковим, то блоки обирати того ж самого розміру, що і при вбудові додаткової інформації);
   - Для кожної пари відповідних блоків з'ясувати:
     - Величину максимального збурення серед *l* СНЧ;
     - Збурення кожного СНВ блоку.

   6.2. Для кожного ЦЗ знайти
   - середнє значення по блоках величини максимального збурення СНЧ;
   - середнє значення збурення кожного СНВ блоку;

   6.3. Для кожної пари множин М1 і $M1_S$, М2 і $M2_S$, М3 і $M3_S$ знайти :
   - середнє значення по блоках величини максимального збурення СНЧ;
   - середнє значення збурення кожного СНВ блоку (для наочності побудувати графіки залежності середнього по блоках збурення лівих, правих СНВ від їх номеру).

   6.4. Для множин $M1 \cup M2 \cup M3$ і $M1_S \cup M2_S \cup M3_S$ знайти:
   - середнє значення по блоках величини максимального збурення СНЧ;
   - середнє значення збурення кожного СНВ блоку (для наочності побудувати графіки залежності середнього по блоках збурення лівих, правих СНВ від їх номеру);
   - дослідити, чи відповідають отримані на практиці результати формальній достатній умові збереженя надійності сприйняття стеганоповідомлення в області сингулярного розкладання.

   6.5. Дослідити відповідність/невідповідність результатів, отриманих за допомогою суб'єктивного ранжирування, різницевого показника і сингулярного розкладання. Пояснити.

7. Зробити висновки про дієвість достатніх умов забезпечення надійності сприйняття стеганоперетворення.
8. Зробити остаточний висновок про ступінь забезпечення надійності сприйняття стеганоалгоритмом *S*. Дослідити, чи є обмеження на область застосування алгоритма *S* (внаслідок наявності можливості незбереження надійності сприйняття стеганоповідомлення). Сформулювати (по можливості) пропозиції щодо удосконалення стеганоалгоритму *S* щодо забезпечення надійності сприйняття стеганоповідомлення.

Варіанти завдання

1. *S* – метод модифікації найменшого значущого біта (реалізація LSB-matching) https://www.researchgate.net/publication/3343443_LSB_matching_revisited ; R - MSE
2. *S* – метод, що використовує різницю значень пікселів (https://www.matec-conferences.org/articles/matecconf/pdf/2016/20/matecconf_icaet2016_02003.pdf стор.3); R – NMSE;
3. *S* – метод випадкового інтервалу (http://pdf.lib.vntu.edu.ua/books/2018/Xoroshko_Komputer_2017_155.pdf стор.64); R - SNR;
4. *S* – метод модифікації найменшого значущого біта (реалізація LSB-replacement) (https://link.springer.com/chapter/10.1007/978-981-15-3172-9_57); R - PSNR;
5. *S* – метод блокового приховування (http://pdf.lib.vntu.edu.ua/books/2018/Xoroshko_Komputer_2017_155.pdf стор.65) ; R - IF;
6. *S* – метод Куттера-Джордана-Боссена (https://studfile.net/preview/7379018/page:33/); R – MSE;
7. *S* – метод Коха і Жао (https://studfile.net/preview/7379018/page:39/); R – NMSE;
8. *S* – метод Бенгама-Мемона-Эо-Юнг (https://studfile.net/preview/7379018/page:40/); R - SNR;
9. *S* – метод, заснований на модифікації максимального сингулярного числа блоку матриці зображення (https://journal.ie.asm.md/assets/files/m71_2_237.pdf стор.99); R - PSNR;
10. *S* – метод, заснований на збуренні яскравості блоку в просторовій області (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=sstt_2014_1_13); R – IF;
11. *S* – метод, заснований на застосуванні LSB в області сингулярного розкладання матриці http://immm.opu.ua/files/archive/n4_v8_2018/immm_n4_v8_2018.pdf стор.368-369); R - MSE
12. *S* – метод, стійкий до масштабування (http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21

REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=sstt_2014_4_5); R – NMSE;

Контрольні запитання

1. Що означає надійність сприйняття стеганоповідомлення?
2. Чи може стеганографічний алгоритм не задовольняти умові збереження надійності сприйняття стеганоповідомлення? Коли це може бути?
3. Яким чином пов’язані кількісні (за допомогою різницевих показників) та якісні (за допомогою суб’єктивного ранжирування) оцінки надійності сприйняття стеганоповідомлення?
4. Який з різницевих показників спотворення ЦЗ, на Ваш погляд, є кращим? Чому?
5. Чи залежить значення різницевого показника від конкретного виду матричної норми, що в ньому використовується?
6. Що можна сказати про дієвість достатніх умов забезпечення надійності сприйняття стеганоперетворення? Яка з достатніх умов є, на Ваш погляд, кращею? Чому? Обгрунтувати теоретично відповідь.
7. Якщо припустити, що стеганоперетворення відбувається в просторовій області ЦЗ, то якою з достатніх умов має сенс користуватися? Чому?
8. Якщо припустити, що стеганоперетворення відбувається в частотній області ЦЗ, то якою з достатніх умов має сенс користуватися? Чому?
9. Пропозиції (по можливості) для удосконалення кількісної оцінки спотворення ЦЗ в результаті збурної дії (не обов’язково стеганоперетворення).

Лабораторна робота №3

Дослідження чутливості стеганоповідомлення до атак проти вбудованого повідомлення

Мета роботи: Застосування загального підходу до аналізу інформаційних систем для встановлення ступеня чутливості до збурних дій стеганоповідомлення, отримуваного різними стеганографічними методами. Дослідження відповідності збурень параметрів повного набору контейнера практичним результатам декодування додаткової інформації в умовах різноманітних атак проти вбудованого повідомлення. Обгрунтування та розробка пропозицій на основі загального підходу до аналізу інформаційних систем до можливого удосконалення (за необхідності) існуючих стеганоалгоритмів з метою покращення їх стійкості до збурних дій.

Лабораторна робота №3 забезпечує у студентів досягнення наступних програмних результатів навчання:

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

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

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

3.1. Чутливість стеганоповідомлення до збурних дій

Одна з основних вимог, що висуваються до будь-якого стеганоповідомлення (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 додаткової інформації (ДІ) й привести до виникнення великої кількості помилок при декодуванні ДІ, і *нечутливим* інакше.

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.

Для стеганоперетворення (СПр) можуть використовуватися як просторова область ЦЗ-контейнера, так і область перетворення. При організації стеганографування, коли мова йде про стійкість розроблювальних методів до різних атак, використовуються, як правило, області перетворення ЦЗ: частотна, області різних розкладань матриці (матриць) ЦЗ-контейнера, хоча деякі алгоритми й намагаються забезпечити робастність шляхом вбудови ДІ в просторовій області ЦЗ.

Переважна більшість стеганоалгоритмів, що позиціонуються як стійкі до атак проти вбудованого повідомлення, зокрема до стиску, здійснюютьвбудову додаткової інформації в частотній області зображення, ґрунтуючись на невірному переконанні, що більш стійкими до різноманітних спотворень є стеганоалгоритми, що використовують для стеганоперетворення саме частотну область. Показано, що властивості стеганоалгоритмів, у тому числі, їх стійкість до збурних дій, визначаються не областю, використовуваною для стеганоперетворення, а величинами й локалізацією збурень сингулярних чисел і сингулярних векторів матриць контейнеру, що відбулися в ході стеганоперетворення (див. лекції 8-12). У зв'язку із цим аналіз стійкості стеганоалгоритма (чутливості формованого їм стеганоповідомлення) може бути проведений в області сингулярного розкладання відповідної матриці, незалежно від того, яка область використовувалася безпосередньо для вбудови ДІ.

3.2. Достатні умови забезпечення нечутливості стеганоповідомлення до збурних дій

Нехай СПр, що здійснюється деяким стеганоалгоритмом, збурило сингулярні вектори (СНВ) матриці контейнера, чи основного повідомлення (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.

Наслідок. Якщо збурені в результаті стеганоперетворення СНВ 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.

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

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

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

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.

Чутливість СП до збурних дій у випадку довільної матриці 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.

Завдання до лабораторної роботи №3

1. Побудувати програмну реалізацію вбудови додаткової інформації в ЦЗ-контейнер шляхом застосування заданого стеганоалгоритму *S*.
2. Для дослідження залежності чутливості/нечутливості стеганоповідомлення, сформованого за допомогою стеганоалгоритму *S*, від формату та якості контейнера сформувати експериментальні множини оригінальних ЦЗ потужністю не менше 100:
    - М1 – ЦЗ у форматі з втратами, обрані з бази зображень;
    - М2 – ЦЗ у форматі без втрат, обрані з бази зображень;
    - М3 – ЦЗ, отримані непрофесійними відеокамерами.
3. Для кожної множини *M1, M2, M3* побудувати відповідні множини стеганоповідомлень $M1_S, M2_S, M3_S$ за допомогою вбудови додаткової інформації стеганоалгоритмом *S,* зберігаючи отримані стеганоповідомлення в форматі без втрат.
4. Кожне ЦЗ-стеганоповідомлення піддати збурній дії D.
5. Декодувати ДІ із збуреного стеганоповідомлення.
6. Общислити значення NC ефективності декодування ДІ.
7. Для кожної множини $M1_S, M2_S, M3_S$ обчислити середнє значення NC.
8. Змінюючи силу збурної дії D шляхом зміни значень параметрів, що її визначають (наприклад, якщо D – гауссовський шум з d=0.0001, то розглянути збурні дії з d=0.001, 0.05, 0.01), і повторюючи кроки 4-7 для нових збурних дій, дослідити, як від сили збурної дії залежить ефективність декодування ДІ в стеганоалгоритмі S. Для наочності побудувати графіки залежності NC від параметру збурної дії для кожної множини $M1_S, M2_S, M3_S$.

9. Порівняти отримані значення NC (отримані на кроці 8 графіки) для множин $M1_S, M2_S, M3_S$. Оцінити стійкість стеганоалгоритму S до збурних дій. Пояснити розбіжність/збіжність NC для різних множин.
10. Побудувати графік залежності NC від параметру збурної дії для множини $M1_S \cup M2_S \cup M3_S$.
11. За результатами, отриманими на кроках 4-10, охарактеризувати ступінь стійкості алгоритму S до збурної дії D.
12. Дослідити, чи задовольняє алгоритм S формальній достатній умові нечутливості формованого стеганоповідомлення до збурних дій, заснованій на аналізі СНЧ і СНВ, для чого:

    Для кожного конкретного ЦЗ:

    - Розбити матриці контейнера та відповідного (незбуреного) стеганоповідомлення на непересічні $l \times l$ –блоки за допомогою стандартної розбивки;
    - Побудувати сингулярні розкладання відповідних $l \times l$ –блоків матриць контейнера та стеганоповідомлення (якщо алгоритм S є блоковим, то блоки обирати того ж самого розміру, що і при вбудові додаткової інформації);
    - Для кожної пари відповідних блоків з'ясувати збурення кожного СНВ блоку.

    Для кожного ЦЗ-контейнера знайти середнє значення збурення кожного СНВ блоку в результаті стеганоперетворення;

    Для кожної пари множин М1 і $M1_S$, М2 і $M2_S$, М3 і $M3_S$ знайти середнє значення збурення кожного СНВ блоку (для наочності побудувати графіки залежності середнього по блоках збурення лівих, правих СНВ від їх номеру).

    Для множин $M1 \cup M2 \cup M3$ і $M1_S \cup M2_S \cup M3_S$ знайти середнє значення збурення кожного СНВ блоку (для наочності побудувати графіки залежності середнього по блоках збурення лівих, правих СНВ від їх номеру; а також графіки залежності середнього по блоках збурення лівих, правих СНВ від відокремленості відповідного СНЧ).

    Дослідити, чи відповідають отримані на практиці результати формальній достатній умові нечутливості стеганоповідомлення до збурної дії D. Пояснити.
13. Зробити остаточний висновок про ступінь чутливості стеганоповідомлення, отриманого стеганоалгоритмом S. Сформулювати (по можливості) пропозиції щодо удосконалення стеганоалгоритму S щодо зменшення чутливості до збурної дії D.

Варіанти завдання

1. S – метод модифікації найменшого значущого біта (реалізація LSB-matching) https://www.researchgate.net/publication/3343443_LSB_matching_revisited
2. S – метод, що використовує різницю значень пікселів (https://www.matec-conferences.org/articles/matecconf/pdf/2016/20/matecconf_icaet2016_02003.pdf стор.3)

3. *S* – метод випадкового інтервалу (http://pdf.lib.vntu.edu.ua/books/2018/Xoroshko_Komputer_2017_155.pdf стор.64)
4. *S* – метод модифікації найменшого значущого біта (реалізація LSB-replacement) (https://link.springer.com/chapter/10.1007/978-981-15-3172-9_57)
5. *S* – метод блокового приховування (http://pdf.lib.vntu.edu.ua/books/2018/Xoroshko_Komputer_2017_155.pdf стор.65)
6. *S* – метод Куттера-Джордана-Боссена (https://studfile.net/preview/7379018/page:33/)
7. *S* – метод Коха і Жао (https://studfile.net/preview/7379018/page:39/)
8. *S* – метод Бенгама-Мемона-Эо-Юнг (https://studfile.net/preview/7379018/page:40/)
9. *S* – метод, заснований на модифікації максимального сингулярного числа блоку матриці зображення (https://journal.ie.asm.md/assets/files/m71_2_237.pdf стор.99)
10. *S* – метод, заснований на збуренні яскравості блоку в просторовій області (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=sstt_2014_1_13)
11. *S* – метод, заснований на застосуванні LSB в області сингулярного розкладання матриці http://immm.opu.ua/files/archive/n4_v8_2018/immm_n4_v8_2018.pdf стор.368-369)
12. *S* – метод, стійкий до масштабування (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=sstt_2014_4_5)

Контрольні запитання

1. Що означає нечутливість стеганоповідомлення до збурних дій?
2. Який стеганоалгоритм називається стійким до атак проти вбудованого повідомлення? Навести приклади таких алгоритмів.
3. Чи може стеганоалгоритм, що виконує вбудову ДІ в просторовій області зображення-контейнера виявитися стійким до атак проти вбудованого повідомлення? Відповідь обгрунтувати.
4. Чи може стеганографічний алгоритм не задовольняти умові стійкості до атак проти вбудованого повідомлення? Коли це може бути? Навести приклад нестійкого алгоритму.
5. Що можна сказати про дієвість достатніх умов забезпечення нечутливості стеганоповідомлення до збурних дій?
6. Якщо припустити, що стеганоперетворення відбувається в частотній області ЦЗ, то якою з достатніх умов має сенс користуватися? Чому?

Література

1. М.М.Браіловський, С.В.Зибін, А.А.Кобозєва, В.О.Хорошко, Ю.Є.Хохлачова. Аналіз кіберзахищеності інформаційних систем. – К.: ФОП Ямчинський О.В., 2021. – 360 с.
2. Кобозєва А.А., Хорошко В.О. Аналіз захищеності інформаційних систем. - К.: Вид. ДУІКТ, 2010. – 316 с.
3. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних підручник. / Г.Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. –558 с.
4. Steganography - The Art of Hiding Information: The Art of Hiding Information. - BoD – Books on Demand, 2024. 160 p.
5. Abid Yahya. Steganography Techniques for Digital Images. Springer, 2018. – 122 p.
6. J.W.Demmel. Applied Numerical Linear Algebra. SIAM. 2001. 430 p.