Міністерство освіти та науки України

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

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

Одесса, 2021

Міністерство освіти та науки України

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

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

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

Одеса, 2021

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 / Укл.: А.А.Кобозєва. – Одеса: «Одеська політехніка», 2021. - 60 с.

Укладач: проф. Кобозєва А.А.

ЗМІСТ

ВСТУП

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.

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 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 розрахована на 2 лабораторних заняття, забезпечує у студентів досягнення наступних програмних результатів навчання:

РН22. 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.

РН24. Використовувати, адаптувати, розвивати сучасні математичні підходи, математичний апарат теорії збурень, матричного аналізу, функцій багатозначної логіки тощо для дослідження процесів, розробки методів та алгоритмів розвязку задач у сфері інформаційної та/або кібербезпеки, зокрема захисту соціотехнічних систем.

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 обумовленоюї, 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, — $\phi\left(\overline{\xi}\right)$. *Числом обумовленості* задачі називається величина, що визначається як:

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

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 представляє 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;

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

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

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

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

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');
```

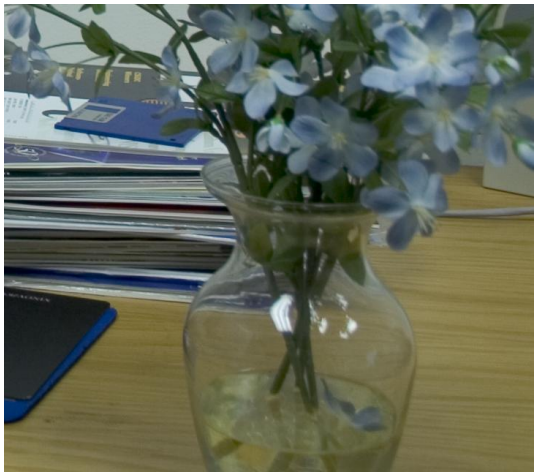
яке піддамо незначній, що є природнім на практиці, збурній дії: накладанню гауссівського шуму з нульовим математичним очікуванням і дисперсією 0.0001:

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

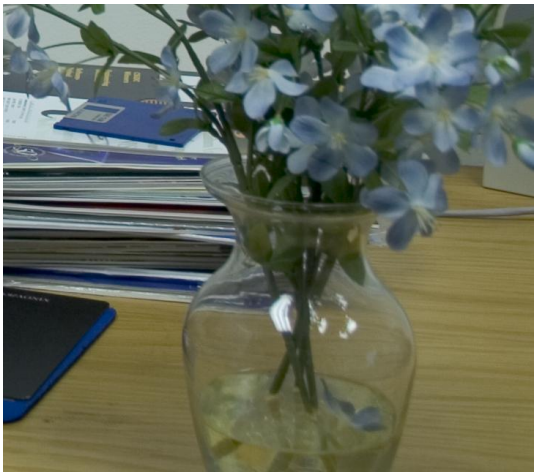
(рис.1.1(б)). З кожного з зображень виділимо одну кольорову складову, наприклад, синю, яку відповідно позначимо *F* і *F1*:

```
>> 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

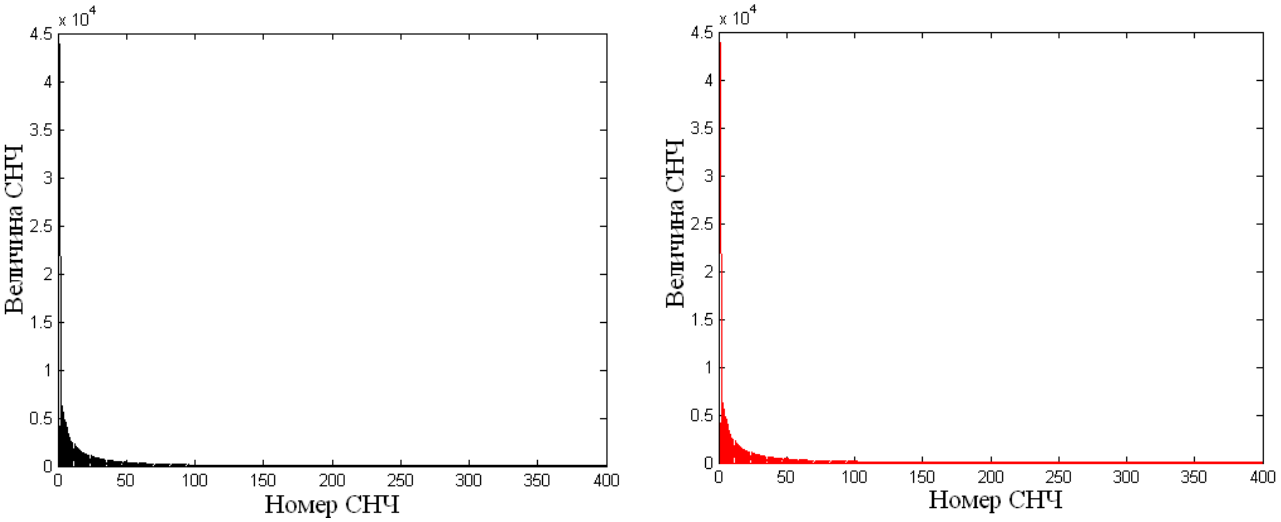
Шляхом побудови сингулярного розкладання обчислимо СНЧ *F* і *F1* , які будуть збережені в діагональних матрицях SIGMA і SIGMA1 відповідно:

```
>> [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

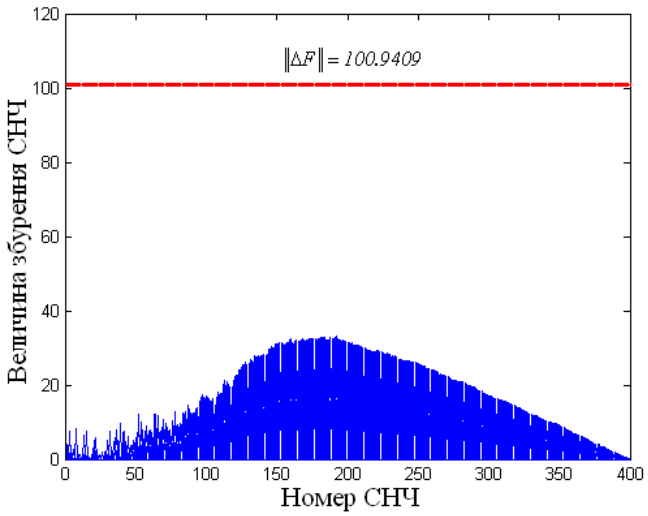


Рис.1.3. Графік залежності збурення СНЧ від його номеру

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.

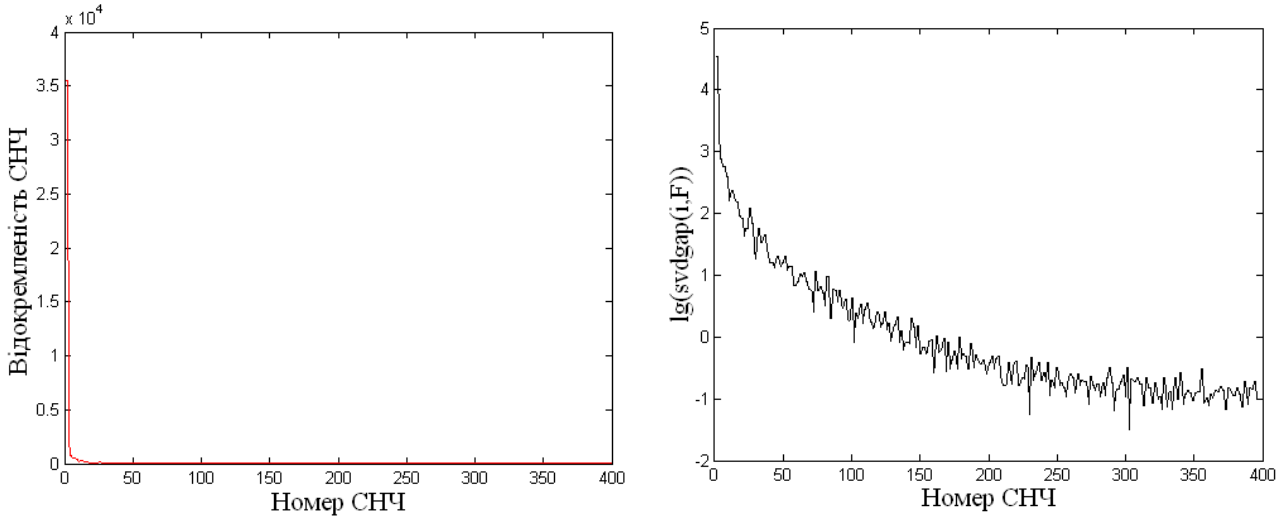
Для СНЧ матриць оригінальних ЦЗ, кадрів цифрового відео співвідношення (1.3) можна уточнити:

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

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.

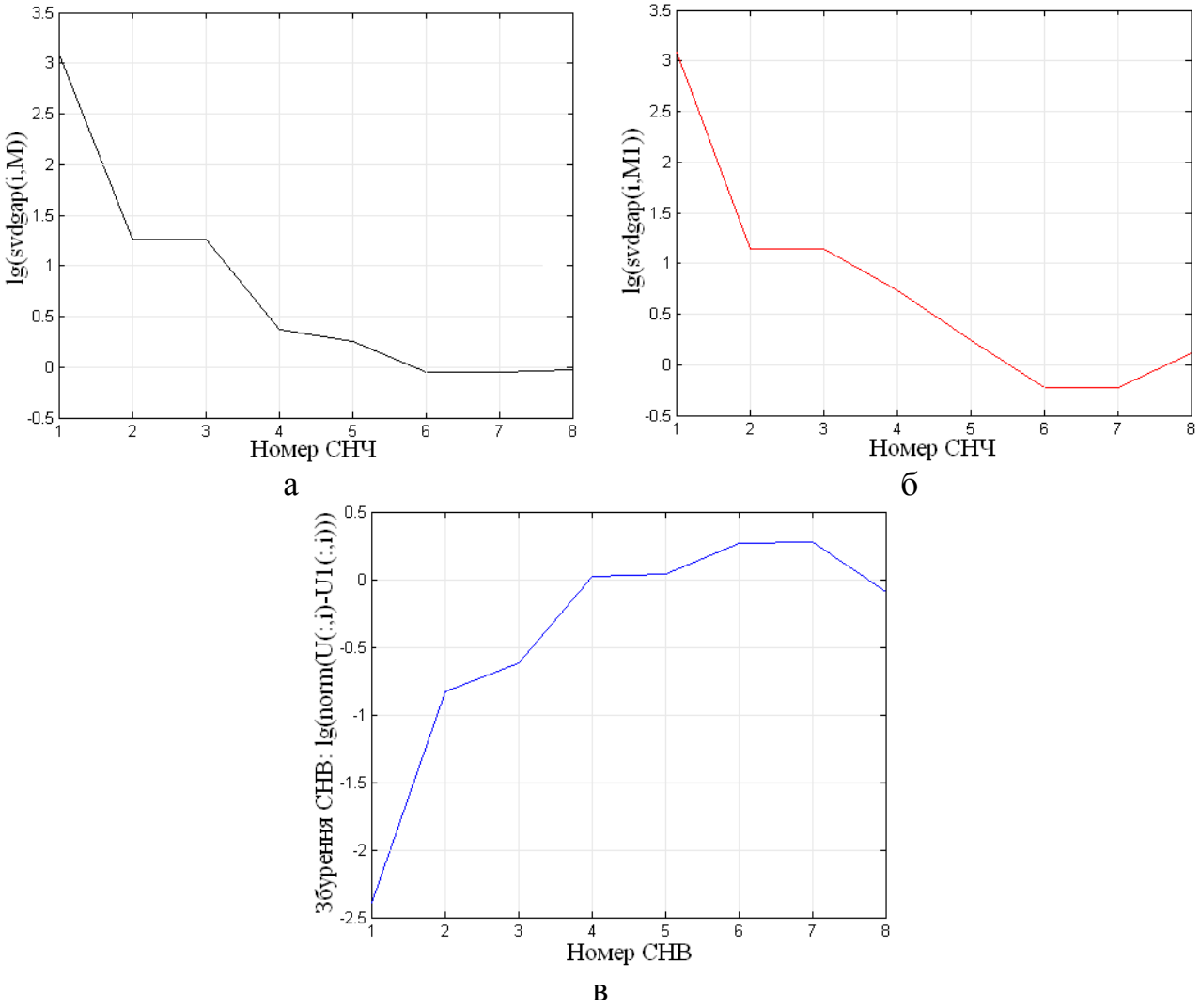


Рис.1.5. Ілюстрація залежності збурення СНВ від відокремленості відповідного СНЧ: а – графік залежності відокремленості СНЧ матриці M від його номеру; б - графік залежності відокремленості СНЧ збуреної матриці M1 від його номеру; в – графік залежності збурення лівого СНВ від його номеру

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:

$$F = U \Lambda U^T \qquad (1.9)$$

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):

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

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:

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

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

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

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

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

— 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:

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

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 в програмному середовищі *Matlab* 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.

Література

1. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.
2. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с.
3. J.W.Demmel. Applied Numerical Linear Algebra. SIAM. 2001. 430 p.

Лабораторна робота №2

Алгоритмічна реалізації універсального методу виявлення порушень цілісності цифрового зображення та дослідження її ефективності

Мета роботи: Розробка алгоритмічної реалізації універсального методу виявлення порушень цілісності цифрового зображення та дослідження її ефективності залежно від розміру блоку цифрового контенту, від сили та специфики (накладаня різноманітних шумів, фільтрація за допомогою різноманітних фільтрів, різноманітні стеганоперетворення тощо) збурної дії. Отримання конкретних рекомендацій по застосуванню метода для різних умов.

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

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН22. 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.

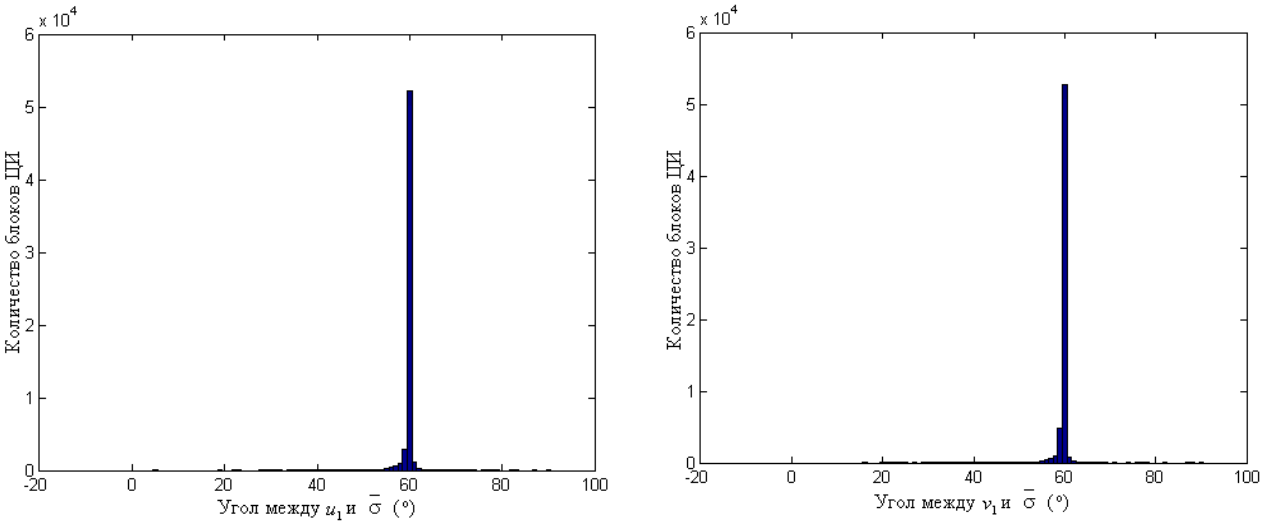
2.1. Аналіз гістограм Γ_U (Γ_V)

Нехай F – матриця цифрового зображення (ЦЗ), яка піддається стандартній розбивці на $l\times l$-блоки, довільний з яких позначимо B.

Теоретично обґрунтовано й практично підтверджено, що величина кута між лівим сингулярним вектором (СНВ) u_1, що відповідає максимальному сингулярному числу (СНЧ) σ_1 і нормованим вектором сингулярних чисел $\bar{\sigma} = \sigma / \|\sigma\|$, де $\sigma = (\sigma_1(B), \sigma_2(B), \ldots, \sigma_l(B))^T \in R^l$ – вектор СНЧ B, $\|\sigma\|$ – норма σ (позначається $\angle(u_1, \bar{\sigma})$), між правим СНВ v_1, що відповідає σ_1, і $\bar{\sigma}$ (позначається $\angle(v_1, \bar{\sigma})$) для більшості блоків оригінального ЦЗ близька до величини кута між n-оптимальним вектором n^O простору R^l, де $n^O = (1/\sqrt{l}, 1/\sqrt{l}, \ldots, 1/\sqrt{l})^T \in R^l$, і першим вектором стандартного базису $e_1 = (1,0,\ldots 0) \in R^l$ (позначається $\angle(n^O, e_1)$):

$$\angle(u_1, \bar{\sigma}) \approx \angle(v_1, \bar{\sigma}) \approx \angle(n^O, e_1). \qquad (2.1)$$

Співвідношення (2.1) характерні для більшості блоків більшості оригінальних ЦЗ. Це дуже чітко і наочно відстежується за допомогою гістограм Γ_U (Γ_V) величин кутів між векторами u_1 і $\bar{\sigma}$ (v_1 і $\bar{\sigma}$) $l\times l$ – блоків, отриманих у результаті стандартної розбивки матриці зображення, де більшість блоків зображення відповідає моді гістограми (рис.2.1 – в випадку блоків розміром 4×4 $\angle(n^O, e_1) = 60^o$).



а б

Рис.2.1. Приклад гістограм значень кутів між векторами u_1 і $\bar{\sigma}$ (а), v_1 і $\bar{\sigma}$ (б) 4×4-блоків в оригінальних ЦЗ

В умовах збурних дій на ЦЗ ці співвідношення часто порушуватися, змінюючи вид гістограм, змінюючи місце розташування моди гістограми (рис.2.2 – мода відповідає 59 градусам).

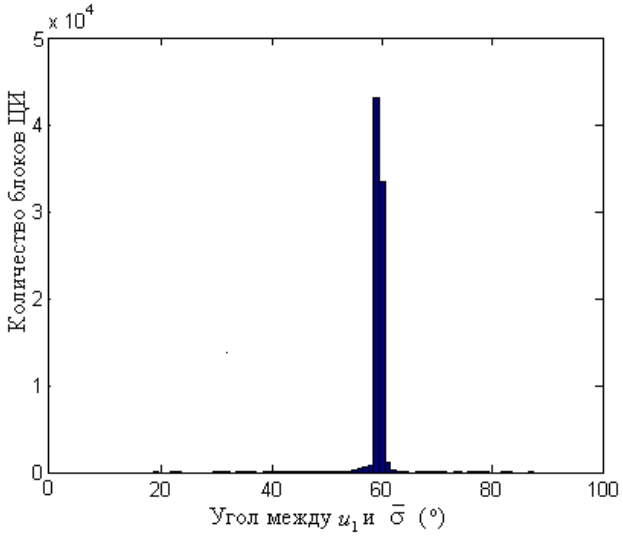


Рис.2.2. Гістограма Γ_U для збуреного ЦЗ, для якого Γ_U оригінального відображена на рис. 2.1 (а)

Однак, з урахуванням лише одного параметра – моди гістограми Γ_U (Γ_V) 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 Γ_U (Γ_V)) ЦЗ.

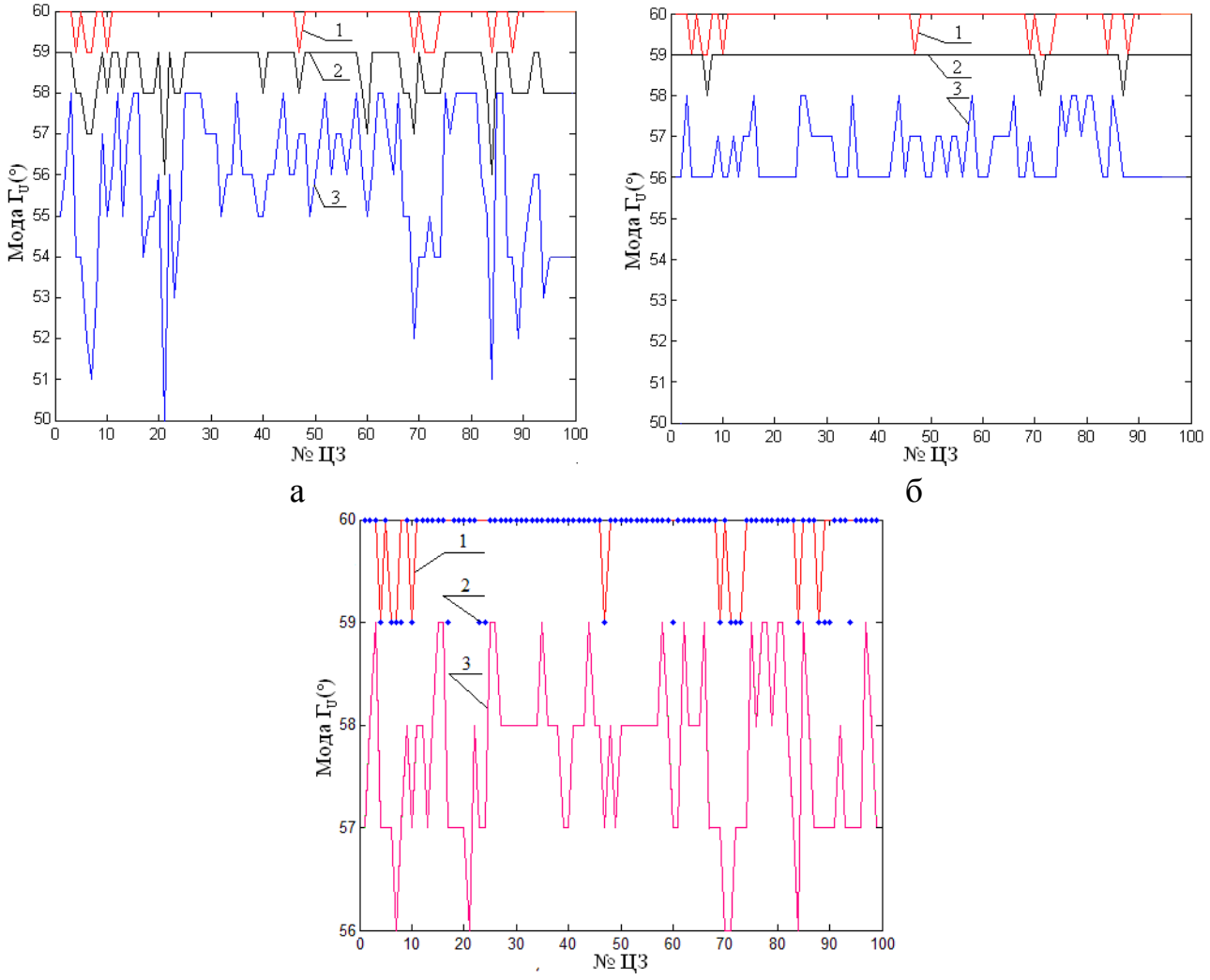


Рис. 2.1. Графіки відповідності моди Γ_U і номера ЦЗ: а –1 – оригінальне ЦЗ; 2 – зашумлене ЦЗ (гауссівський шум з нульовим математичним очікуванням і $D = 0.001$); 3 – зашумлене ЦЗ (гауссівський шум з нульовим математичним очікуванням і $D = 0.01$); б – 1 – оригінальне ЦЗ; 2 – зашумлене ЦЗ (мультиплікативний 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)

Якщо (2.1) буде мати місце для збуреного ЦЗ, то результат збурення формально відобразиться в зменшенні значення глобального максимуму Γ_U (Γ_V) для збуреного ЦЗ, в порівнянні з оригінальним і, як наслідок, в «розширенні» самої гістограми в околі моди Γ_U (Γ_V) (рис.4.1), яке кількісно може бути оцінено за допомогою відношення кількості блоків зображення, для яких $\angle\left(u_1, \overline{\sigma}\right)$ ($\angle\left(v_1, \overline{\sigma}\right)$) знаходиться в малому околі $\angle\left(n^O, e_1\right)$, до значення гістограми Γ_U (Γ_V) в моді: чим більше значення вказаного відношення, тим більше ймовірність того, що зображення, що піддається експертизі, є таким, цілісність якого порушена.

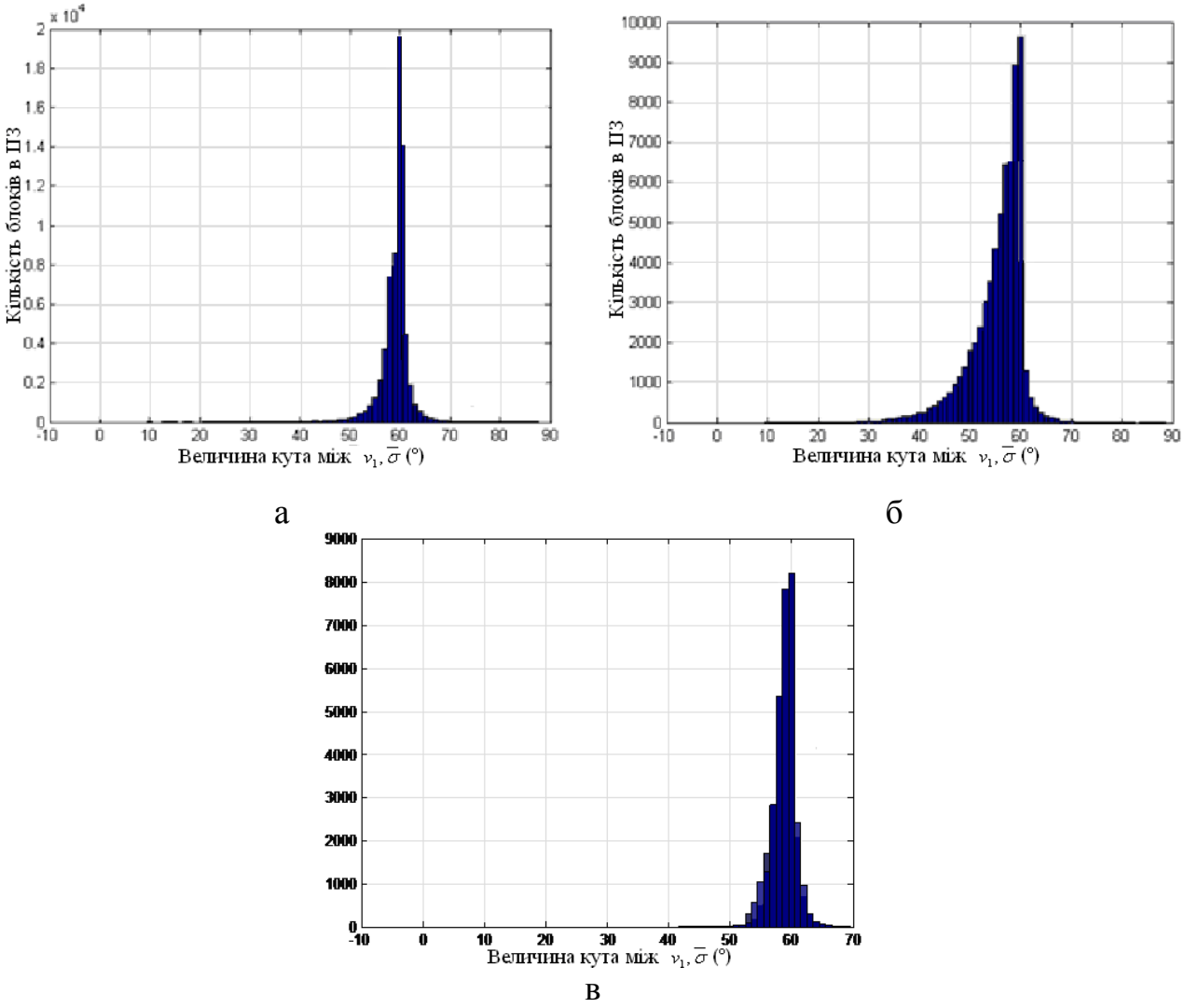


Рис. 4.1. Гістограми Γ_V (для блоків 4×4) конкретного ЦЗ (формат Tif): а – оригінальне ЦЗ; б – ЦЗ після накладання гауссівського шуму з нульовим математичним очікуванням і D = 0.001); в – ЦЗ-стеганоповідомлення, сформоване стеганографічним методом LSB з пропускною спроможністю прихованого каналу зв'язку 0.75 біт/піксель

2.2. Метод виявлення порушення цілісності та його алгоритмічна реалізація

Крок 1. З аналізованого ЦЗ виокремлюється кольорова складова *K*, яка розбивається стандартним чином на $l \times l$-блоки.

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

Крок 3. Для аналізованого ЦЗ побудувати гістограми Γ_U, Γ_V з кроком *h*.

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

Крок 5. Для аналізованого ЦЗ з використанням Γ_U, Γ_V обчислити відповідно кількості S_U, S_V блоків, для яких $\angle\left(u_1, \bar{\sigma}\right) \in \left[\angle\left(n^O, e_1\right) - T, \left(n^O, e_1\right) + T\right]$, $\angle\left(v_1, \bar{\sigma}\right) \in \left[\angle\left(n^O, e_1\right) - T, \angle\left(n^O, e_1\right) + T\right]$, де T – параметр, що визначається експериментально.

Крок 6 (*перевірка*).

Якщо

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

то

для аналізованого ЦЗ цілісність порушена.

Якщо

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

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

то

для аналізованого ЦЗ цілісність порушена.

Якщо

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

то

для аналізованого ЦЗ цілісність не порушена.

Рекомендовано: В алгоритмі методу використати наступні значення параметрів: $T = 15^o$, $P_U = P_V = 3.2$.

2.3. Аналіз ефективності методу

Ефективність алгоритмічної реалізації виявлення порушень цілісності ЦЗ може оцінюватися за допомогою наступних параметрів:

- помилки I-го роду (ЦЗ, цілісність якого порушена, визначається як оригінальне),
- II-го роду (оригінальне ЦЗ визначається як таке, цілісність якого порушена),

Дуже часто, зокрема в зарубіжних наукових статтях, використовується інший кількісний показник ефективності: точність виявлення порушення цілісності (*accuracy* (*ACC*)):

$$ACC = (TP + TN)/(TP + FN + TN + FP), \qquad (2.2)$$

де *TP* (*True Positive*) — число правильно виявлених ЦЗ, цілісність яких була порушена (істинопозитивний результат); *TN* (*True Negative*) — число правильно виявлених оригінальних ЦЗ (істинонегативний результат); *FP* (*False Positive*) — число оригінальних ЦЗ, помилково прийнятих за такі, цілісність яких була порушена (хибнопозитивний результат (хибна тривога) або помилка II роду); *FN* (*False Negative*) — число ЦЗ, цілісність яких була порушена, помилково визнаних оригінальними (хибнонегативний результат або помилка I роду). Цей показник є більш зручним з точки зору можливості проведення порівняльного аналізу ефективності з існуючими аналогами.

Завдання до лабораторної роботи №2

1. На прикладі конкретного ЦЗ дослідити якісні і кількісні властивості гістограм Γ_U (Γ_V), побудованих з кроком в 1 градус, для оригінального зображення і зображень, отриманих в результаті трьох різних збурних дій на подане оригінальне (це може бути фільтрація, накладання шуму, стеганоперетворення тощо). Пояснити отримані результати. Чи відповідають отримані результати очікуваним?

2. Розробити програмну реалізацію алгоритму універсального методу виявлення порушень цілісності цифрового зображення.
3. Для дослідження залежності/незалежності ефективності алгоритму, що розглядається, від формату та якості ЦЗ 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.
4. Для кожної множини *M1, M2, M3* побудувати відповідні множини ЦЗ $M1_D, M2_D, M3_D$, цілісність яких порушена в результаті збурної дії D.
5. Дослідити ефективність алгоритму універсального методу виявлення порушень цілісності цифрового зображення залежно від формату оригінального ЦЗ та розміру l використовуваного при аналізі ЦЗ $l \times l$-блоку в умовах конкретної збурної дії D, для чого:
   5.1. Отримати помилки 1-го та 2-го роду для кожної пари відповідних експериментальних множин ЦЗ: $M1_D \; i \; M1, M2_D \; i \; M2, M3_D \; i \; M3$ для кожного з запропонованих в Вашому варіанті завдання розміру блоку l; визначити *ACC* (2.2).
   5.2. Для кожної пари відповідних експериментальних множин ЦЗ побудувати графіки залежності ефективності алгоритму (*ACC*) від l.
   5.3. Дослідити, як залежить ефективність алгоритму від формату та якості досліджуваних ЦЗ.
   5.4. Отримати помилки 1-го та 2-го роду, *ACC* для відповідних експериментальних множин $M1 \cup M2 \cup M3$ і $M1_D \cup M2_D \cup M3_D$. Побудувати графік залежності ефективності алгоритму (*ACC*) від l.
   5.5. Проаналізувати співвіднесення графіків, отриманих на кроках 5.2, 5.4.
6. Змінити параметри збурної дії D. Нова збурна дія D_1. Проробити крок 5 в умовах D_1.
7. Дослідити, чи взагалі алгоритм є ефективним в застосовуваних умовах. Якщо ні, дослідити причини.
8. Отримати рекомендації по використанню алгоритма відносно розмірів блоку в умовах обраної збурної дії.
9. Дослідити залежність ефективності алгоритму від значення параметра T (параметр змінювати в малому околі 15 градусів). Проаналізувати отримані результати з точки зору необхідності уточнення експериментально визначеного параметру T.
10. По можливості, обгрунтувати та внести пропозиції по підвищенню ефективності універсального методу виявлення порушень цілісності цифрового зображення.
11. ***Додаткове завдання***.
    - Дослідити, яким чином впливає крок гістограм Γ_U, Γ_V на ефективність алгоритму;
    - Провести порівняльний аналіз ефективності реалізованого алгоритму з існуючими аналогами (з відкритих джерел).

Варіанти завдань

1. K=B; $l \in \{4,8,16\}$; D - гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.001; D_1 - гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.01.
2. K=G; $l \in \{4,8,16\}$; D - мультиплікативний шум з d=0.001; D_1 - мультиплікативний шум з d=0.01.
3. K=R; $l \in \{4,12,24\}$; D - гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.001; D_1 - гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.01.

4. К=B; $l \in \{4,12,24\}$; D - мультиплікативний шум з d=0.001; D_1 - мультиплікативний шум з d=0.01.
5. К=B; $l \in \{4,8,16\}$; D – шум «сіль-перець» з d=0.02; D_1 - шум «сіль-перець» з d=0.04.
6. К=R; $l \in \{4,12,24\}$; D – шум «сіль-перець» з d=0.02; D_1 - шум «сіль-перець» з d=0.04.
7. К=B; $l \in \{4,16,32\}$; D - мультиплікативний шум з d=0.0001; D_1 - мультиплікативний шум з d=0.001.
8. К=R; $l \in \{4,16,32\}$; D - гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.0001; D_1 - гауссівський шум з нульовим математичним очікуванням та дисперсією d=0.001.
9. К=G; $l \in \{4,16,32\}$; D – стеганоперетворення за допомогою LSB-методу з пропускною спроможністю прихованого каналу звязку 0.5 біт/піксель; D_1 - стеганоперетворення за допомогою LSB-методу з пропускною спроможністю прихованого каналу звязку 1 біт/піксель.
10. К=B; $l \in \{4,8,16\}$; D – стеганоперетворення за допомогою LSB-методу з пропускною спроможністю прихованого каналу звязку 0.75 біт/піксель; D_1 - стеганоперетворення за допомогою LSB-методу з пропускною спроможністю прихованого каналу звязку 1 біт/піксель.
11. К=B; $l \in \{4,8,16\}$; D відповідає матриці збурення, яку сформувати самостійно; $D_1 = 2D$.
12. К= G; $l \in \{4,8,12\}$; D відповідає матриці збурення, яку сформувати самостійно; $D_1 = 1.5D$.

Контрольні запитання

1. Які переваги, недоліки мають універсальні методи виявлення порушення цілісності цифрових контентів?
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. Пояснити наближену рівність (2.1).
5. Чи впливає конкретика збурної дії (що відрізняється від стиску з втратами) якісно на характер зміни гістограми збуреного ЦЗ в порівнянні з оригінальним? Чому?
6. Як Ви вважаєте, при збільшенні сили збурної дії на оригінальне ЦЗ, збільшиться чи зменшиться ефективність розглянутого алгоритму по виявленню порушення цілісності? Відповідь пояснити.

Література

1. Кобозєва А.А. Основи загального підходу до розробки універсальних стеганоаналітичних методів для цифрових зображень. *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

Лабораторна робота №3

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 №3 забезпечує у студентів досягнення наступних програмних результатів навчання:

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН24. Використовувати, адаптувати, розвивати сучасні математичні підходи, математичний апарат теорії збурень, матричного аналізу, функцій багатозначної логіки тощо для дослідження процесів, розробки методів та алгоритмів розвязку задач у сфері інформаційної та/або кібербезпеки, зокрема захисту соціотехнічних систем.

3.1. 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.

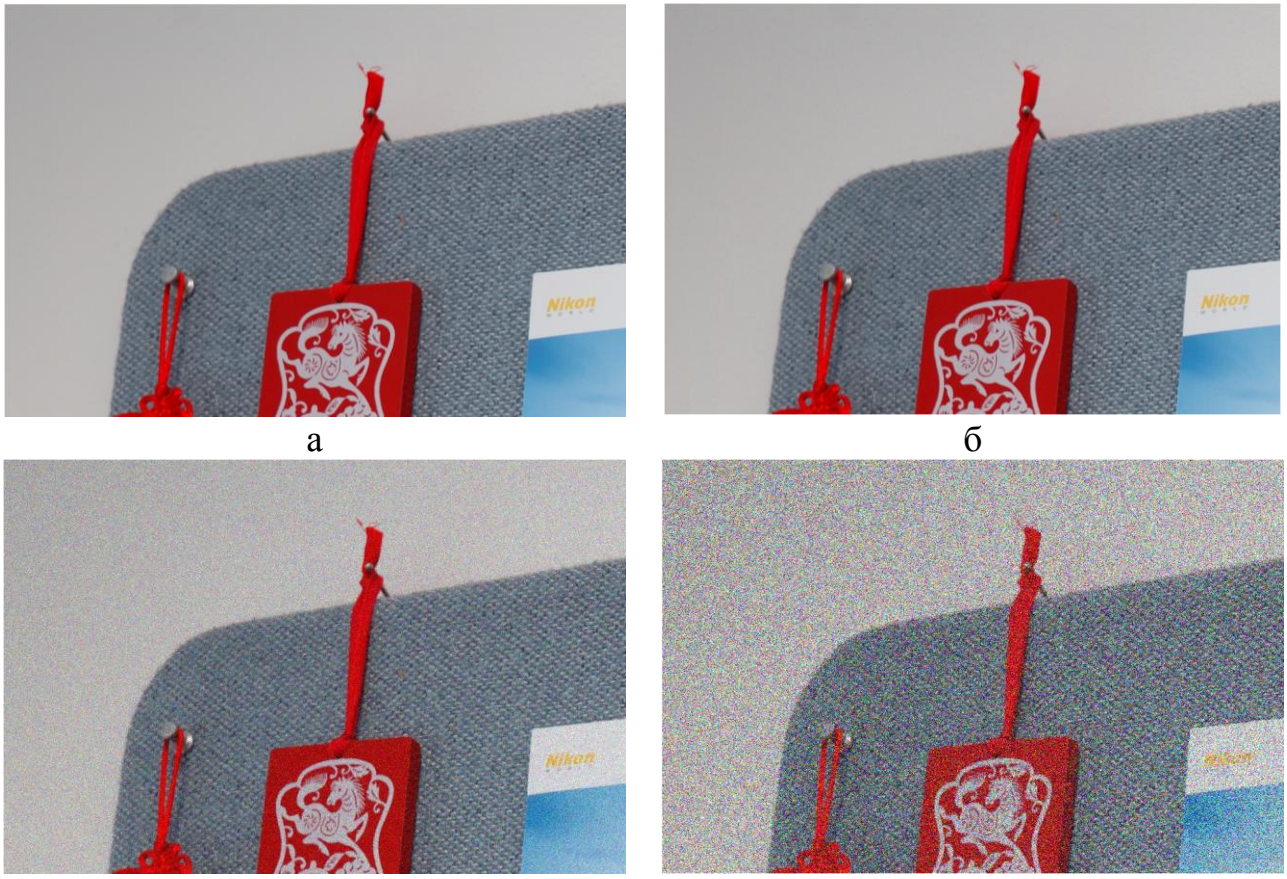
Довільне СПр представляється у вигляді збурення СНЧ і (або) СНВ матриці ОП, що визначаються нормальним сингулярним розкладанням матриці.

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.3.1 для оригінального ЦЗ (рис.3.1(а)) розміром 666×1002 пікселя, норма червоної кольорної складової якого становить 3.1830e+007. Норма матриці збурення становила 2.1467e+005 (рис.3.1(б)), 2.1344e+006 (рис.3.1(в)), 6.3776e+006 (рис.3.1(г)).



а б

в г

Рис.3.1. Ілюстрація залежності надійності сприйняття ЦЗ від норми матриці збурення

Шляхом субєктивного ранжирування встановлено, що надійність сприйняття для ЦЗ (рис.3.1(б)) не порушена, чого не можна сказати про два інші збурені ЦЗ (рис.3.1(в,г)).

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

Розглядається ОП з довільною матрицею F.

1. Нехай вбудова ДІ викликає збурення $\delta_{k_1},\ldots,\delta_{k_p}$ СНЧ $\sigma_{k_1},\ldots,\sigma_{k_p}$ 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.3.2, 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.3.3 – збурення зазнали СНВ блоків матриці ЦЗ, отриманих шляхом стандартної розбивки, що відповідають максимальним СНЧ блоків (з максимальними відокремленостями)).

а б

Рис.3.2. Ілюстрація збереження надійності сприйняття ЦЗ при незначних збуреннях СНЧ: а – оригінальне ЦЗ; б – збурене ЦЗ

а б

Рис.3.3. 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.

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

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

$$V = YH_N,$$

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

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

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

Двовимірне дискретне перетворення Уолша-Адамара визначається як

$$W = H'_N X H'^T_N, \qquad (3.1)$$

де $H'_N = \frac{1}{N} H_N$, 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). Найбільший інтерес для встановлення умови дотримання надійності сприйняття СП представляє локалізація образів високочастотних складових матриці X ЦЗ.

Кожна з функцій Уолша (рядок матриці H_N), не будучи гармонійною, характеризується частостю, яка визначається наступним чином. 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 (табл.1).

Таблиця 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

Частость функції УА відіграє ключову роль при отриманні достатньої умови збереження надійності сприйняття СП. У матриці (3.1), 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

(3.1), 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 (рис.3).

(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. 3. Відповідність трансформант УА коефіцієнтам ДКП для блоків різного розміру $l \times l$: а – l=4; б – l=8; в – l=16;

Область можливого збурення блоків ЦЗ в області перетворення Уолша-Адамара, що дає можливість збереження надійності сприйняття СП, можна розширити шляхом всановлення відповідності між трансформантами УА і сингулярними тройками матриці (рис. 5).

(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. 5. Локалізація області можливого збурення в результаті СПр в області перетворення Уолша-Адамара для $l \times l$-блоків ЦЗ: а – l=4; б – l=8; в – l=16

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. 5 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 A.

3.4. 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 №3

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. Дослідити, чи задовольняє алгоритм *S* формальній достатній умові збереження надійності сприйняття стеганоповідомлення в області перетворення Уолша-Адамара, для чого:

7.1. Для кожного конкретного ЦЗ:
- Розбити матриці контейнера та стеганоповідомлення на непересічні $l \times l$ – блоки за допомогою стандартної розбивки;
- Побудувати перетворення УА 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 обчислити збурення трансформант УА.

7.2. Для кожного ЦЗ знайти середні значення по блоках збурень трансформант УА його блоків.

7.3. Для кожної пари множин М1 і $M1_S$, М2 і $M2_S$, М3 і $M3_S$ знайти середні значення по блоках збурень трансформант УА для ЦЗ, що входять до цих пар множин (для наочності для кожної пари множин побудувати графіки залежності середнього по блоках збурення трансформанти УА від її індексів (*i*,*j*) (для цього матрицю трансформант можна представити у вигляді вектора)).

7.4. Для множин $M1 \cup M2 \cup M3$ і $M1_S \cup M2_S \cup M3_S$ знайти середні значення по блоках збурень трансформант УА для всіх ЦЗ, задіяних в експерименті (для наочності побудувати графіки залежності середнього по блоках збурення трансформанти УА від її індексів (*i*,*j*)).

7.5. Дослідити, чи відповідають отримані на практиці результати формальній достатній умові збереженя надійності сприйняття стеганоповідомлення в області перетворення УА.

7.6. Дослідити відповідність/невідповідність результатів, отриманих за допомогою суб'єктивного ранжирування, різницевого показника і перетворення УА. Пояснити.

8. Порівняти результати, отримані на кроках 6,7. Зробити висновки про дієвість достатніх умов забезпечення надійності сприйняття стегаоперетворення.
9. 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=&S21REF=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).

Література

1. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.
2. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с.
3. J.W.Demmel. Applied Numerical Linear Algebra. SIAM. 2001. 430 p.

Лабораторна робота №4

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 №4 забезпечує у студентів досягнення наступних програмних результатів навчання:

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН24. Використовувати, адаптувати, розвивати сучасні математичні підходи, математичний апарат теорії збурень, матричного аналізу, функцій багатозначної логіки тощо для дослідження процесів, розробки методів та алгоритмів розвязку задач у сфері інформаційної та/або кібербезпеки, зокрема захисту соціотехнічних систем.

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.

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 стеганоперетворенні 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 №4

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

4. *S* – метод модифікації найменшого значущого біта (реалізація LSB-matching) https://www.researchgate.net/publication/3343443_LSB_matching_revisited
5. *S* – метод, що використовує різницю значень пікселів (https://www.matec-conferences.org/articles/matecconf/pdf/2016/20/matecconf_icaet2016_02003.pdf стор.3)
6. *S* – метод випадкового інтервалу (http://pdf.lib.vntu.edu.ua/books/2018/Xoroshko_Komputer_2017_155.pdf стор.64)
7. *S* – метод модифікації найменшого значущого біта (реалізація LSB- replacement) (https://link.springer.com/chapter/10.1007/978-981-15-3172-9_57)
8. *S* – метод блокового приховування (http://pdf.lib.vntu.edu.ua/books/2018/Xoroshko_Komputer_2017_155.pdf стор.65)

9. *S* – метод Куттера-Джордана-Боссена (https://studfile.net/preview/7379018/page:33/)
10. *S* – метод Коха і Жао (https://studfile.net/preview/7379018/page:39/)
11. *S* – метод Бенгама-Мемона-Эо-Юнг (https://studfile.net/preview/7379018/page:40/)
12. *S* – метод, заснований на модифікації максимального сингулярного числа блоку матриці зображення (https://journal.ie.asm.md/assets/files/m71_2_237.pdf стор.99)
13. *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)
14. *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)
15. *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. Кобозєва А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем.- К.: Вид. ДУІКТ, 2010. – 316 с.
2. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с.
3. J.W.Demmel. Applied Numerical Linear Algebra. SIAM. 2001. 430 p.

Лабораторна робота №5

Методи детектування фотомонтажу, клонування, проведеному в цифровому зображенні

Мета роботи: Застосування методів, заснованих на загальному підході до аналізу інформаційних систем, або інших існуючих методів шляхом їх алгоритмічної та наступної програмної реалізації для виявлення результатів порушення цілісного цифрового зображення шляхом фотомонтажу або клонування. Дослідження ефективності застосованих методів (алгоритмів) залежно від розміру неоригінальної області зображення, а також в умовах додаткових збурних дій. Обгрунтування та розробка пропозицій до можливого удосконалення (за необхідності) існуючих методів з метою підвищення їх ефективності.

Лабораторна робота №5 забезпечує у студентів досягнення наступних програмних результатів навчання:

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН22. 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.

РН24. Використовувати, адаптувати, розвивати сучасні математичні підходи, математичний апарат теорії збурень, матричного аналізу, функцій багатозначної логіки тощо для дослідження процесів, розробки методів та алгоритмів розвязку задач у сфері інформаційної та/або кібербезпеки, зокрема захисту соціотехнічних систем.

Робота передбачає виконання її групою студентів по 5-6 чоловік.

5.1. Локальні порушення цілісності цифрового зображення

Локальні порушення цілісності цифрових контентів, коли збурення оригінального контенту відбувається лише у межах якоїсь (невеликої) області (областей), не змінюючи інші його частини, є дуже поширеними.

Локальні зміни на практиці для ЦЗ мають місце, як правило, внаслідок фотомонтажу або клонування. З урахуванням наявності й доступності сучасних графічних редакторів (Adobe Photoshop, Gimp та ін.) такі операції легко й якісно реалізуються навіть непрофесіоналами, роблячи актуальною задачу виявлення таких порушень, яка на сьогоднішній день залишається невирішеною повною мірою.

При фотомонтажі використовуються частини декількох ЦЗ, композиція яких утворює нове ЦЗ. Найчастіше при фотомонтажі одне ЦЗ розглядається як основне, або базове. Додавання частин іншого (інших) зображення локально заміняє його оригінальні області на «чужі» (рис.5.1). Розв'язок задачі виявлення фотомонтажу тут чітко вказує на область локального порушення цілісності базового ЦЗ.

Одним з найбільш широко й часто використовуваних програмних інструментів при неавторизованих змінах ЦЗ є клонування, реалізоване у всіх сучасних графічних редакторах. При клонуванні область зображення, що називається прообразом, копіюється й вставляється в іншу область цього ж зображення, заміняючи собою його оригінальну частину й утворюючи клон прообразу. Описана процедура часто використовується у випадку, коли з ЦЗ усувається «небажаний» об'єкт, змінюється взаємне розташування об'єктів, дублюється об'єкт/об'єкти (рис.5.2-5.4).

В результаті виявлення результатів клонування визначаються області клону (де відбулося порушення цілісності ЦЗ) й оригінального прообразу (КП) (рис.5.5), причому, як правило, без відокремлення однієї від іншої, тому тут, на відміну від фотомонтажу, виявлення області локального порушення цілісності фактично не відбувається.

а

б

в

г

Рис. 5.1. Ілюстрація застосування для ЦЗ фотомонтажу: а, б – оригінальні ЦЗ; в – результат проведеного фотомонтажу; г – результат виявлення фотомонтажу

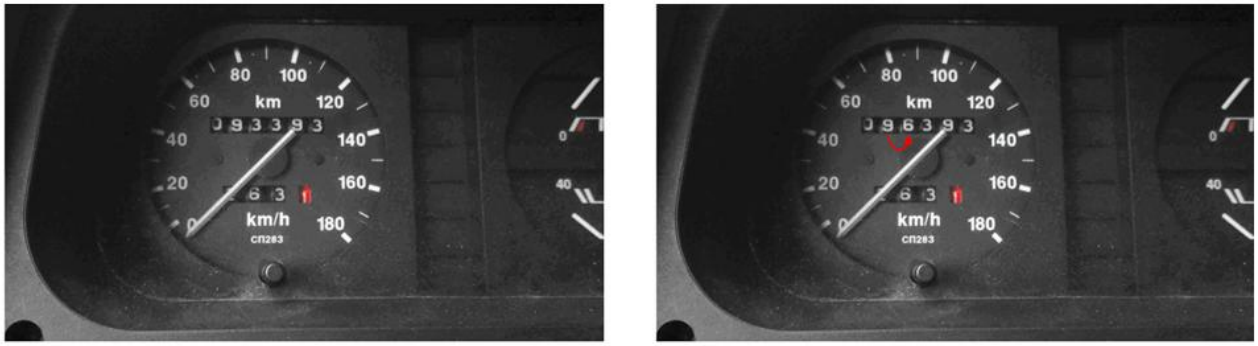
а

б

Рис.5.2. Ілюстрація застосування клонування з метою усунення об’єкту з ЦЗ: а – Оригінальне ЦЗ; б – результат клонування

а б

Рис.5.3. Застосування клонування з метою дублювання об’єкту: а – оригінальне ЦЗ; б - результат клонування



а б

Рис.5.4. Ілюстрація проведення клонування з метою зміни взаємного розташування об'єктів: а – оригінальне ЦЗ; б - результат клонування

Рис.5.5. Результат виявлення клонування для ЦЗ, наведеного на рис.5.4 (б)

5.2. Порівняння основних підходів до виявлення результатів клонування

Методи виявлення результатів клонування в ЦЗ мають різноманітні математичні базиси, при цьому пасивна технологія для виявлення КП тут може бути розділена на два основних великих класи методів: блокові методи (*block-based methods*) і методи, засновані на аналізі ключових точок (*keypoint-based methods*).

Основна ідея блокових методів, що мають, як правило, значну обчислювальну складність, полягає в тому, що ЦЗ розбивається на пересічні/непересічні області/блоки, після чого зображення аналізується не цілком, а окремими отриманими після розбивки частинами, серед яких шукаються співпадаючі або порівнянні по певних ознаках. Блоково-орієнтований

підхід знайшов своє відображення в численних розробках сучасних фахівців в області інформаційної безпеки.

На основі аналізу літературних джерел можна стверджувати, що блокові методи, як правило, мають значну обчислювальну складність, аналізуючи непересічні/пересічні блоки ЦЗ, яке піддається експертизі, що є їхнім основним недоліком, однак вони дозволяють виявляти області КП навіть в умовах їх малих розмірів.

На відміну від блоково-орієнтованих, алгоритми, засновані на аналізі характерних точок ЦЗ, як правило, працюють із зображенням цілком, не розбиваючи його на підобласті, блоки. Використовувані характеристики відносяться до всього зображення, що підвищує ефективність обчислень і робить цю групу методів кращими в порівнянні із блоково-орієнтованими з погляду обчислювальної складності. Двома основними типами таких методів є SIFT (*Scale Invariant Features Transform*) і SURF (*Speed UP Robust Features*). Основна ідея методів даної групи полягає у виділенні ключових точок ЦЗ (підобласті ЦЗ). Ці методи можуть виявитися неефективними у випадку, коли клонування використовується з метою видалення якогось (можливо малого за розмірами) об'єкта із частини зображення, що має незначний перепад значень яскравості пікселів, а також просто в умовах малих розмірів КП, для яких пошук ключових точок може викликати утруднення.

Таблиця 5.1 – Порівняння блоково-орієнтованого підходу й підходу, заснованого на аналізі ключових точок для виявлення результатів клонування в ЦЗ

Блоково-орієнтований підхід	***Підхід, заснований на аналізі ключових точок зображення***
Розбивка зображення на блоки для виділення характерних ознак	Без розбивки зображення визначення ключових точок для виділення характерних ознак
Потрібно більше пам'яті й більший час обчислення, ніж в підході, заснованому на аналізі ключових точок ЦЗ	Оскільки кількість ключових точок менше кількості блоків, то потрібно менше пам'яті й часу обчислень
Більш точне виявлення областей клону й прообразу	Менш точне виявлення областей клону й прообразу
Чутливість методів до розмірів області клону/прообразу	
Необеспечение достаточной эффективности в условиях додаткових збурних дій	

Вибір підходу, методу для виявлення результатів фотомонтажу, клонування, ефективність цього виявлення залежить від конкретних умов, в яких відбулося локальне порушення цілісності ЦЗ.

Завдання до лабораторної роботи №5

1. Сформувати експериментальну множину M оригінальних ЦЗ потужністю не менше 100.
2. Сформувати експериментальну множину $\overline{M}$ неоригінальних (таких, цілісність яких порушена шляхом клонування або фотомонтажу) ЦЗ потужністю не менше 100 (для цього можна скористатися існуючими базами таких зображень, наприклад, CoMoFoD https://www.researchgate.net/publication/266927943_CoMoFoD_-New_Database_for_Copy-Move_Forgery_Detection , чи сформувати множину самостійно).
3. Обрати метод (алгоритм) S виявлення результатів фотомонтажу чи клонування. Побудувати програмну реалізацію S.
4. Провести дослідження ефективності роботи S в умовах відсутності/наявності додаткової постобробки спотвореного (тобто такого, яке зазнало операції клонування чи фотомонтажу) ЦЗ. В якості постобробки можуть розглядатися: стиск спотвореного ЦЗ з втратами, корекція його кольору, яскравості, розмиття спотвореного ЦЗ тощо. Для цього:

Для ЦЗ з множини M визначити показник *FPR:*

$$FPR = \frac{кількість\ оригінальних\ ЦЗ, виявлених\ як\ такі, що\ зазнали\ клонування}{загальна\ кількість\ оригінальних\ ЦЗ} \cdot 100\%$$

Для ЦЗ з множини $\overline{M}$ визначити показник *TPR:*

$$TPR = \frac{кількість\ ЦЗ, що\ зазнали\ клонування, виявлених\ як\ клоновані}{загальна\ кількість\ ЦЗ, що\ зазнали\ клонування} \cdot 100\%;$$

зробити висновок про ефективність алгоритму в умовах відсутності додаткової постобробки ЦЗ.

ЦЗ з множини $\overline{M}$ піддати збурним діям D1 (з параметрами d_1, d_2, d_3, які будуть змінювати силу збурної дії), D2 отримуючи множини $\overline{M}_{11}$, $\overline{M}_{12}$, $\overline{M}_{13}$, $\overline{M}_2$ відповідно.

Для ЦЗ з множин $\overline{M}_{11}$, $\overline{M}_{12}$, $\overline{M}_{13}$ визначити показник *TPR*. Побудувати графік залежності *TPR* від сили збурної дії (параметру збурної дії). Зробити висновок про ефективність алгоритму в умовах наявності додаткової постобробки ЦЗ (збурна дія D1), про залежність/незалежність ефективності алгоритму від сили збурної дії D1. Пояснити.

Для ЦЗ з множини $\overline{M}_2$ визначити показник *TPR*. Зробити висновок про ефективність алгоритму в умовах наявності додаткової постобробки ЦЗ (збурна дія D2).

5. Спланувати та виконати експериментальні дослідження залежності/незалежності ефективності алгоритму S від розміру області порушення цілісності.
6. Сформувати рекомендації по умовам використання алгоритму S.
7. Сформувати (по можливості) пропозиції щодо удосконалення S з метою підвищення його ефективності.

Варіанти

В якості методу для виявлення фотомонтажу взяти, наприклад,

- https://www.researchgate.net/publication/311957994_Digital_image_forgery_detection_techniques_a_survey ;
- https://www.tandfonline.com/doi/full/10.1080/00450618.2016.1153711?scroll=top&needAccess=true ;
- https://www.researchgate.net/publication/220646137_Digital_image_splicing_detection_based_on_approximate_run_length ;
- https://www.sciencedirect.com/science/article/abs/pii/S0031320312002440 ;
- https://www.researchgate.net/publication/301408175_SVD-based_image_splicing_detection ;
- http://suchasnaspetstehnika.com/journal/ukr/2017_2/4.pdf

або будь-який інший метод.

В якості методу для виявлення клонування взяти, наприклад,

- https://www.researchgate.net/publication/245568958_Fast_and_Robust_Forensics_for_Image_Region-duplication_Forgery
- https://www.researchgate.net/publication/269308369_A_review_on_copy_move_image_forgery_detection_techniques
- https://pubmed.ncbi.nlm.nih.gov/20832208/
- https://ieeexplore.ieee.org/document/5582232
- https://ieeexplore.ieee.org/document/5734842
- https://www.researchgate.net/publication/284296608_Detection_of_Region_Duplication_Forgery_in_Digital_Images_Using_SURF

або будь-який інший метод.

1. D1 – стиск з втратами (Jpeg), параметр – коефіцієнт якості QF ($d_1 : QF = 90$, $d_2 : QF = 75$, $d_3 : QF = 65$); D2 – накладання шуму «сіль-перець».

2. D1 – стиск з втратами (Jpeg), параметр – коефіцієнт якості QF ($d_1 : QF = 85$, $d_2 : QF = 75$, $d_3 : QF = 60$); D2 – накладання мультиплікативного шуму.
3. D1 – стиск з втратами (Jpeg), параметр – коефіцієнт якості QF ($d_1 : QF = 90$, $d_2 : QF = 75$, $d_3 : QF = 45$); D2 – накладання гауссовського шуму.

Контрольні запитання

1. Чим принципово відрізняються задачі виявлення клонування і фотомонтажу? Яка задача Вам здається більш складною? Чому?
2. Чому важливим є дослідження алгоритму виявлення результатів клонування, фотомонтажу в умовах стиску спотвореного ЦЗ з втратами? Яким коефіцієнтам якості треба приділити основну увагу? Чому?
3. З я кою метою на практиці застосовується постобробка ЦЗ після клонування, фотомонтажу? Які саме методи постобробки використовуються тут найчастіше?
4. Що можна сказати про характеристики тих збурних дій, які можуть використовуватися для постобробки ЦЗ після клонування, фотомонтажу? Відповідь пояснити.
5. На які групи розподіляються всі методи виявлення клонування ЦЗ? Чому?
6. Області клону якого розміру можуть ефективно виявлятися сучасними методами? Як Ви вважаєте, чи достатньо цього на практиці?

Література

1. 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.
2. 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.
3. Nor Bakiah AbdWarif, Ainuddin Wahid AbdulWahab, Mohd Yamani IdnaIdris, 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
4. 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
5. 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
6. 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
7. 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

Лабораторна робота №6

Методи виявлення обробки цифрового зображення засобами графічних редакторів

Мета роботи: Застосування методів, заснованих на загальному підході до аналізу інформаційних систем, або інших існуючих методів шляхом їх алгоритмічної та наступної програмної реалізації для виявлення результатів порушення цілісного цифрового зображення шляхом обробки засобами графічних редакторів (розмиття, корекція яскравості, кольору тощо). Дослідження ефективності застосованих методів (алгоритмів) залежно від параметрів, що використовуються під час обробки. Обгрунтування та розробка пропозицій до можливого удосконалення (за необхідності) існуючих методів з метою підвищення їх ефективності.

Лабораторна робота №6 забезпечує у студентів досягнення наступних програмних результатів навчання:

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН22. 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.

РН24. Використовувати, адаптувати, розвивати сучасні математичні підходи, математичний апарат теорії збурень, матричного аналізу, функцій багатозначної логіки тощо для дослідження процесів, розробки методів та алгоритмів розвязку задач у сфері інформаційної та/або кібербезпеки, зокрема захисту соціотехнічних систем.

Робота передбачає виконання її групою студентів по 5-6 чоловік.

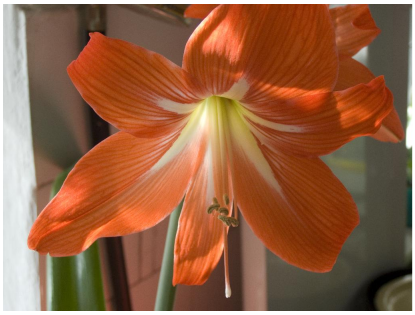
Порушення цілісності цифрових зображень засобами графічних редакторів

Відомі й широко використовувані графічні редактори, такі як Adobe Photoshop, GIMP і інші пропонують різноманітні інструменти для обробки зображень, коли зображення або його частини зазнають таким операціям, як зміна масштабу (рис.6.1), поворот (рис.6.2), розмиття, зміна яскравості (рис.6.3), кольору й т.п., а результат цих операцій без наявності оригінального ЦЗ візуально може і не ідентифікуватися.

Для захисту й виявлення такої обробки створюються відповідні методи й алгоритми, які підрозділяються на дві великі категорії: активні й пасивні.

В активних методах деяка інформація попередньо вбудовується в ЦЗ (цифровий водяний знак (ЦВЗ), цифровий підпис (ЦП)). Суттєвим недоліком активних методів є те, що при використанні ЦВЗ інформація, що вбудовується, повинна бути занурена в цифровий об'єкт безпосередньо під час створення цього об'єкта, що обмежує область застосування методів тільки для механізмів генерації ЦЗ, що мають вбудовані можливості занурення ЦВЗ, чого більша частина широко використовуваних фотоапаратів на сьогоднішній день ще не має, а при використанні ЦП необхідно зберігати цифровий підпис еталонного зображення.

а



б

Рис.6.1. Масштабування ЦЗ з використанням засобів графічного редактору: а – оригінальне ЦЗ; б – результат масштабування ЦЗ з коефіцієнтом 0.5

а

б

в

Рис. 6.2. Поворот ЦЗ з використанням засобів графічного редактору: а – оригінальне ЦЗ; б – результат повороту ЦЗ на кут 5 градусів за годинниковою стрілкою; в – результат обрізання ЦЗ після повороту

а б

Рис.6.3. Зміна яскравості ЦЗ: а – оригінальне ЦЗЖ б – ЦЗ, для якого яскравість зменшена

Перерахованих вище недоліків позбавлені пасивні методи, які дозволяють підтвердити цілісність ЦЗ або виявити її порушення без впровадження додаткової інформації. Пасивні методи розподіляються на дві категорії:

- з ідентифікацією вихідного обладнання;
- виявлення спотворень в аналізованому зображенні.

Методи першої категорії дозволяють визначити, чи є ЦЗ отриманим безпосередньо після зйомки камерою, або в ньому були зроблені якісь зміни графічними редакторами або іншими програмами. Коли камера створює ЦЗ, вона зберігає його зі своїми особливостями (Exif-дані), властивими саме цій камері. При зміні ЦЗ змінюються й Exif-дані. Exif-дані зберігають інформацію про камеру, наприклад, про фокусну відстань, про те, чи використовувався спалах, коли був зроблений знімок, і т.і. Камери також можуть зберігати координати, де було знято фото (при наявності вбудованого приймача GPS).

До першої категорії можна віднести, наприклад, методи, що працюють із цифровою звуковою інформацією. Вхідними даними в таких методах є цифрові звукові файли довільного змісту, для яких припускається, що вони записані на наданій апаратурі. Шляхом аналізу наявного цифрового звукового файлу визначається, чи дійсно на наданій апаратурі звукозапису був зроблений запис даного файлу й чи є даний запис первинним. Для аналізу зі звукового файлу виділяються й досліджуються такі статистичні характеристики, які пов'язані з апаратурою звукозапису, як апаратурна перешкода. У результаті аналізу виявляється факт і місця монтажу в представленому цифровому звуковому файлі за умови, що монтаж здійснювався компіляцією фрагментів цифрових звукових файлів, записаних на різній апаратурі.

Недоліком методів категорії з ідентифікацією вихідного обладнання є наявність таких інструментів, які дозволяють редагувати ЦЗ, не змінюючи їх змісту. До таких інструментів можна віднести, наприклад, зміну яскравості або контрасту, розрізання зображення й т.і. А також дані методи дозволяють зробити висновок про можливе редагування ЦЗ, але не визначають область і характер внесених спотворень, що робить методи, віднесені до другої категорії, такими, що мають переваги.

Завдання до лабораторної роботи №6

1. Сформувати експериментальну множину *M* оригінальних ЦЗ потужністю не менше 100. Обрати метод (алгоритм) S виявлення обробки цифрового зображення засобами графічних редакторів. Нехай цей алгоритм спрямований на виявлення обробки D (розмиття, стиску з втратами, накладання шуму тощо) ЦЗ.
2. Сформувати експериментальні множини $\overline{M}_1$, $\overline{M}_2$, $\overline{M}_3$ неоригінальних (таких, цілісність яких порушена шляхом застосування до них обробки D з різними параметрами d_1, d_2, d_3, які будуть змінювати силу збурної дії) ЦЗ, зберігаючи їх в форматі без втрат.
3. Побудувати програмну реалізацію *S*.
4. Провести дослідження ефективності роботи *S*. Для цього:
   - Для ЦЗ з множини M визначити показник *FPR;*
   - Для ЦЗ з множин $\overline{M}_1$, $\overline{M}_2$, $\overline{M}_3$ визначити показник *TPR*. Побудувати графік залежності *TPR* від сили збурної дії (параметру збурної дії). Зробити висновок про ефективність алгоритму, про залежність/незалежність ефективності алгоритму від сили збурної дії D. Пояснити.
   - Для ЦЗ з множини $\overline{M}_1$ Y $\overline{M}_2$ Y $\overline{M}_3$ визначити показник *TPR*. Зробити загальний висновок про ефективність алгоритму.
5. Спланувати та виконати експериментальні дослідження залежності/незалежності ефективності алгоритму S від формату збереження ЦЗ після його обробки засобами графічних редакторів.
6. Сформувати рекомендації по умовам використання алгоритму S.
7. Сформувати (по можливості) пропозиції щодо удосконалення S з метою підвищення його ефективності.

Варіанти

В якості методу S виявлення обробки ЦЗ засобами графічних редакторів, наприклад, можна взяти:

- 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=Znpviknu_2013_44_19 ;
- 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_2013_3_6
- https://cyberleninka.ru/article/n/primenenie-metodov-otsenivaniya-razmytosti-tsifrovyh-izobrazheniy-v-zadache-audiovizualnogo-monitoringa
- http://immm.opu.ua/files/archive/n1-2_v9_2019/immm_n1-2_v9_2019.pdf (стор.49-58)
- http://immm.opu.ua/files/archive/n1-2_v10_2020/immm_n1-2_v10_2020.pdf (стор.61-67)
- http://immm.opu.ua/files/archive/n1-2_v11_2021/immm_n1_2_v11_2021.pdf (стор.48-55)
- 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=riu_2017_2_17
- 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=Znpviknu_2019_63_11

або будь-який інший з існуючих методів.

Контрольні запитання

1. Чому, на Ваш погляд, виявлення обробки ЦЗ засобами графічних редакторів є важливою задачею з точки зору інформаційної безпеки?
2. Для чого використовується на практиці обробка ЦЗ засобами графічних редакторів?
3. Яким чином застосовується загальний підхід до аналізу стану інформаційних систем в задачах, пов’язаних з виявленням результатів обробки ЦЗ засобами графічних редакторів? Які саме параметри з повного набору використовуються тут? Чому?
4. Яку роль відіграє обробка ЦЗ засобами графічних редакторів в умовах клонування, фотомонтажу, стеганографічного каналу зв’язку? Пояснити?

Література

1. 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.
2. В.В. Зоріло, О.Ю. Лебедєва, Н.О. Бензар. Розробка алгоритму виявлення зашумлення як фальсифікації цифрового зображення. – ІМММ. – 2021. – Т.11, №1-2.
3. В.В. Зоріло, О.А. Карпова. Алгоритм виявлення обробки цифрового зображення фільтром «Motion blur». – ІМММ, 2019. – Т.9, №1-2. – С. 49-58.