DOI 10.15276/imms.v12.no3.162
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 162-172

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ПЕРЕТВОРЕНИХ БЛОКІВ ЦИФРОВОГО ЗОБРАЖЕННЯ ДЛЯ ВИЯВЛЕННЯ ПОРУШЕННЯ ЙОГО ЦІЛІСНОСТІ

І.І. Бобок

Національний університет «Одеська Політехніка»,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

Проблема виявлення порушення цілісності інформаційного контенту є одною з основних проблем сучасної інформаційної безпеки. Несанкціоноване змінений інформаційний контент при його використанні з нерозважальною метою може привести до критично негативних наслідків як для окремих людей, підприємств, банків, фірм, так і до катастрофічних наслідків для людства в цілому, якщо кібератаки будуть спрямовані на сферу військової галузі, енергетики, хімічної промисловості тощо. Світова наукова спільнота приділяє багато уваги проблемі виявлення порушень цілісності інформаційних контентів, зокрема цифрових зображень, що розглядаються в роботі, але остаточного розв'язку ця проблема не має, задача удосконалення підходів та методів експертизи цілісності цифрових контентів залишається актуальною. Метою роботи є дослідження можливостей удосконалення існуючого підходу до виявлення несанкціонованих змін цифрових зображень, заснованого на аналізі сингулярних чисел і сингулярних векторів блоків відповідної матриці, шляхом дослідження властивостей блоків, отриманих з використанням різноманітних перетворень, що відрізняються від запропонованих раніше. Досліджені властивості блоків, отриманих шляхом загальної симетризації, а також шляхом запропонованих перетворень, результатом яких є несиметричні матриці, що можуть використовувати довільну кількість m матриць-множників. Встановлено, що для підвищення ефективності підтвердження збереження цілісності зображення має сенс використовувати симетризовані блоки при m=2, несиметризовані - при m=3, але з урахуванням пріоритетності виявлення саме порушення цілісності в загальному випадку перевагу треба віддати перетворенню симетризації з m=2.

Ключові слова: цілісність цифрового зображення, порушення цілісності, сингулярне число, сингулярний вектор, чутливість до збурюючих дій.

Вступ

Проблема виявлення порушення цілісності інформаційного контенту є одною з основних проблем сучасної інформаційної безпеки [1,2]. Несанкціоновано змінений інформаційний контент при його використанні з нерозважальною метою може привести до критично негативних наслідків як для окремих людей, підприємств, банків, фірм в вигляді компрометації персональних даних, матеріального, економічного збитку [3,4], так і до катастрофічних наслідків для людства в цілому, якщо кібератаки будуть спрямовані на сферу військової галузі, енергетики, хімічної промисловості тощо, що може поставити під загрозу життя людей в усьому світі. Інформація на сьогоднішній день стає найдорожчим і найзатребуванішим товаром [5].

Світова наукова спільнота приділяє багато уваги проблемі виявлення порушень цілісності інформаційних контентів, зокрема цифрових зображень (ЦЗ), що відбуваються в результаті різноманітних збурних дій [6-8], але остаточного розв'язку ця проблема не має. Більше того, на погляд автора, вона принципово взагалі не може бути вирішеною остаточно, оскільки розвиток інформаційних технологій, теорії інформаційної безпеки приводе до удосконалення способів та методів, що використовуються для несанкціонованих змін контентів, а методи виявлення – це, як правило, відповідь на нові «виклики». Тому задача

удосконалення підходів та методів експертизи цілісності цифрових контентів, зокрема ЦЗ, що і розглядаються в роботі, сьогодні і завтра залишаться актуальними.

Нещодавно в роботах [9-14] був запропонований новий підхід до вирішення проблеми виявлення порушення цілісності ЦЗ/кадрів цифрового відео, заснований на аналізі властивостей сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) $l\times l$-блоків матриці цифрового контенту, отриманих шляхом стандартної розбивки його матриці [15], що є результатом нормального сингулярного розкладання [10]:

$$B = U\Sigma V^T, \quad (1)$$

де B – $l\times l$-блок, U, V – ортогональні $l\times l$-матриці, стовпці яких $u_1,\ldots,u_l$ і $v_1,\ldots,v_l$ – відповідно ліві (лексикографічно додатні) і праві СНВ B, $\Sigma = diag\left(\sigma_1(B),\ldots,\sigma_l(B)\right)$, $\sigma_1(B)\geq\ldots\geq\sigma_l(B)\geq 0$ – СНЧ B.

В межах підходу було первісно встановлено [9-10], що для більшості блоків більшості оригінальних ЦЗ має місце співвідношення:

$$\angle\left(u_1,\bar{\sigma}\right)\approx\angle\left(v_1,\bar{\sigma}\right)\approx\angle\left(n^O,e_1\right), \quad (2)$$

де $\bar{\sigma}=\sigma/\|\sigma\|$, $\sigma=\left(\sigma_1(B),\sigma_2(B),\ldots,\sigma_l(B)\right)^T\in R^l$ – вектор СНЧ B, $\|\sigma\|$ – норма σ, $\angle\left(u_1,\bar{\sigma}\right)$, $\angle\left(v_1,\bar{\sigma}\right)$ - величини кутів між векторами u_1 і $\bar{\sigma}$, v_1 і $\bar{\sigma}$ відповідно, $n^O=\left(1/\sqrt{l},1/\sqrt{l},\ldots,1/\sqrt{l}\right)^T\in R^l$ - n-оптимальний вектор простору R^l, $e_1=(1,0,\ldots,0)\in R^l$ - перший вектор стандартного базису R^l, $\angle\left(n^O,e_1\right)$ - кут між векторами n^O,e_1.

Удосконалення підходу [11-14] привело до встановлення факту, що співвідношення

$$\angle\left(u_1,\bar{\bar{\sigma}}\right)\approx\angle\left(v_1,\bar{\bar{\sigma}}\right)\approx\angle\left(n^O,e_1\right), \quad (3)$$

де $\bar{\bar{\sigma}}=\left(\sigma_1^2(B),\sigma_2^2(B),\ldots,\sigma_l{}^2(B)\right)^T\Big/\left\|\left(\sigma_1^2(B),\sigma_2^2(B),\ldots,\sigma_l{}^2(B)\right)^T\right\|$, виконується для більшості блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, при цьому рівність в (3) має місце для більшої кількості блоків більшої кількості оригінальних ЦЗ, ніж в (2).

Згаданий підхід добре зарекомендував себе при застосуванні в задачах стеганоаналізу, зокрема універсального, при виявленні результатів накладання різноманітних шумів, розмиття ЦЗ, виявленні блокової обробки, локальних порушень цілісності зображення тощо. Враховуючи це, а також те, що результати його роботи при реалізації в конкретних експертних методах не є абсолютними, тобто такими, що взагалі не можна покращити, актуальним є питання удосконалення цього підходу для підвищення ефективності відповідних експертних методів, що на ньому базуються.

Метою роботи є дослідження можливостей удосконалення підходу виявлення порушень цілісності ЦЗ, заснованого на аналізі СНЧ і СНВ блоків матриці ЦЗ, шляхом дослідження властивостей блоків, отриманих з використанням перетворень, що відрізняються від запропонованих раніше [11-14].

Основний матеріал

Перетвореннями блоку B, що використовувалися при удосконаленні [11-14] експертного підходу, заснованому на аналізі СНЧ і СНВ блоків матриці ЦЗ, були дві симетризації у вигляді:

$$B\to BB^T,\ B\to B^TB,$$

які приводили до підвищення ефективності експертизи цілісності, в порівнянні з аналізом параметрів поданого блоку B, завдяки тому, що СНЧ $\sigma_i\left(BB^T\right)$, $\sigma_i\left(B^TB\right)$,

$i=\overline{1,l}$, матриць BB^T, B^TB відрізнялися від СНЧ B відповідно до співвідношення: $\sigma_i\left(BB^T\right)=\sigma_i\left(B^TB\right)=\sigma_i^{\,2}(B)$, а СНВ BB^T, B^TB, що одночасно були і власними векторами, співпадали з лівими, правими СНВ B відповідно.

Симетризація блоку в загальному вигляді може бути представлена наступним чином:

$$B\to BB^TBB^T...BB^T,\qquad B\to B^TBB^TB...B^TB, \tag{4}$$

де кількість множників-матриць в правих частинах перетворень (4) дорівнює $2k$, $k\in N$, N – множина натуральних чисел. Дійсно, якщо є деяка симетрична матриця $A=A^T$, то множення її на себе довільну кількість разів залишить результуючу матрицю симетричною: $\left(AA...A\right)^T=A^TA^T...A^T=AA...A$. В нашому випадку: $A=BB^T$, $A=B^TB$. Виникає питання: чи приведе до наступного покращення експертного підходу аналіз блоків ЦЗ, отриманих за допомогою перетворень (4) з $k>1$?

Твердження 1. Для матриць (4) мають місце наступні співвідношення:

$$\sigma_i\left(BB^T...BB^T\right)=\sigma_i\left(B^TB...B^TB\right)=\sigma_i^{\,2k}\left(B\right),i=\overline{1,l}, \tag{5}$$

ліві і праві СНВ матриці $BB^TBB^T...BB^T$, що одночасно є її власними векторами, співпадають з лівими СНВ матриці B, а ліві і праві СНВ матриці $B^TBB^TB...B^TB$, що одночасно є її власними векторами, співпадають з правими СНВ матриці B.

Доказ. Покажемо, що для матриці $BB^TBB^T...BB^T$ має місце наступне співвідношення:

$$\underbrace{BB^TBB^T...BB^T}_{2k\ множників}=U\Sigma^{2k}U^T. \tag{6}$$

Скористаємося для цього принципом математичної індукції. Використовуючи (1), для k=1 отримаємо:

$$BB^T=U\Sigma^2U^T. \tag{7}$$

Припустимо, що для деякого $k=n$ рівність (6) доведена, тобто $\underbrace{BB^TBB^T...BB^T}_{2n\ множників}=U\Sigma^{2n}U^T$. Перевіримо (6) для $k=n+1$, використовуючи припущення індукції і (7):

$$\underbrace{BB^TBB^T...BB^T}_{2(n+1)\ множників}=\underbrace{BB^TBB^T...BB^T}_{2n\ множників}BB^T=U\Sigma^{2n}U^TBB^T=U\Sigma^{2n}U^TU\Sigma^2U^T=U\Sigma^{2(n+1)}U^T.$$

Таким чином, співвідношення (6) має місце для $\forall k\in N$.

Аналогічним чином, використовуючи рівність, отриману за допомогою (1):

$$B^TB=V\Sigma^2V^T, \tag{8}$$

можна показати, що для матриці $B^TBB^TB...B^TB$ має місце наступне співвідношення:

$$\underbrace{B^TBB^TB...B^TB}_{2k\ множників}=V\Sigma^{2k}V^T. \tag{9}$$

Співвідношення (6), (9), враховуючи властивості матриць U,V,Σ, визначених для (1), є нормальними спектральними (одночасно і сингулярними) розкладаннями для матриць $BB^TBB^T...BB^T$, $B^TBB^TB...B^TB$ відповідно, з чого випливає рівність (5) і висновок твердження для їх СНВ.

Відповідність між СНЧ поданої і перетвореної матриці блоку B, аналогічна (5), буде мати місце і в випадку перетворень матриці виду:

$$B\to BB^TBB^T...BB^TB,\qquad B\to B^TBB^TB...B^TBB^T, \tag{10}$$

де кількість множників-матриць в правих частинах перетворень (10) дорівнює $2k$+1, $k\in N$. Для (10) має місце наступне твердження.

Твердження 2. Для матриць (10) мають місце співвідношення:

$$\sigma_i\left(BB^T...BB^TB\right)=\sigma_i\left(B^TB...B^TBB^T\right)=\sigma_i^{\,2k+1}(B),\ \ i=\overline{1,l}\,, \tag{11}$$

ліві і праві СНВ матриці $BB^TBB^T...BB^TB$ співпадають відповідно з лівими і правими СНВ матриці B, а ліві і праві СНВ матриці $B^TBB^TB...B^TBB^T$ співпадають з правими і лівими СНВ матриці B відповідно.

Доказ. Аналогічно доказу твердження 1 з використанням співвідношень (7), (8) та наступних, отриманих з урахуванням (1): $BB^TB=U\Sigma^3V^T$, $B^TBB^T=V\Sigma^3U^T$.

Позначимо вектори СНЧ матриць $BB^TBB^T...BB^T$, $B^TBB^TB...B^TB$, $B^TBB^TB...B^TBB^T$, $BB^TBB^T...BB^TB$ наступним чином:

$$\sigma_{B^TB...B^TB}=\left(\sigma_1\left(B^TB...B^TB\right),...,\sigma_l\left(B^TB...B^TB\right)\right)^T=\left(\sigma_1^{2k}(B),...,\sigma_l^{\,2k}(B)\right)^T=\sigma_{BB^T...BB^T}=\sigma_{(B)^{(2k)}}$$

$$\sigma_{B^TB...B^TBB^T}=\left(\sigma_1\left(B^TB...B^TBB^T\right),...,\sigma_l\left(B^TB...B^TBB^T\right)\right)^T=\left(\sigma_1^{2k+1}(B),...,\sigma_l^{\,2k+1}(B)\right)^T=\sigma_{BB^T...BB^TB}=\sigma_{(B)^{(2k+1)}}$$

В блоках оригінального ЦЗ має місце співвідношення:

$$\sigma_1(B)>>\sigma_2(B)\geq...\geq\sigma_l(B)\geq 0\,. \tag{12}$$

При піднесенні до ступеня $2k/2k+1$ СНЧ B при обчисленні СНЧ матриць (4), (10) відповідно до (5), (11) зменшаться малі (менші 1) і збільшаться великі (більші 1) значення, ще більше відокремивши максимальне СНЧ від усіх інших. При нормуванні векторів $\sigma_{(B)^{(2k)}}$, $\sigma_{(B)^{(2k+1)}}$, результатом чого буде вектор

$$\bar{\sigma}^{(2k)}=\sigma_{(B)^{(2k)}}\Big/\left\|\sigma_{(B)^{(2k)}}\right\|,\ \bar{\sigma}^{(2k+1)}=\sigma_{(B)^{(2k+1)}}\Big/\left\|\sigma_{(B)^{(2k+1)}}\right\|,$$

перші компоненти $\bar{\sigma}^{(2k)}$, $\bar{\sigma}^{(2k+1)}$ виявляться ближчими до одиниці, ніж перші компоненти вектора $\bar{\sigma}$, а останні можуть виявитися значно ближче до 0, ніж останні компоненти $\bar{\sigma}$, що приводить до наступного твердження, що є узагальненням висновків, представлених в [11,14].

Твердження 3. Для блоків оригінального ЦЗ, отриманих в результаті стандартної розбивки його матриці, має місце співвідношення

$$\angle\left(e_1,\bar{\sigma}^{(p)}\right)<\angle\left(e_1,\bar{\sigma}^{(m)}\right)<\angle\left(e_1,\bar{\sigma}\right), \tag{13}$$

якщо $p>m$.

Доказ. Нехай $\alpha=\angle\left(e_1,\bar{\sigma}\right)$, тоді [11,14]:

$$cos\,\alpha=\frac{\sigma_1(B)}{\sqrt{\sigma_1^{\,2}(B)+\sigma_2^{\,2}(B)+...+\sigma_l^{\,2}(B)}}\,.$$

Нехай $\beta_m=\angle\left(e_1,\bar{\sigma}^{(m)}\right)$. Тоді

$$cos\,\beta_{(m)}=\frac{\sigma_1^{\,m}(B)}{\sqrt{\sigma_1^{\,2m}(B)+\sigma_2^{\,2m}(B)+...+\sigma_l^{\,2m}(B)}}\,. \tag{14}$$

Права частина (13) при $m>1$ випливає з відповідного твердження [11,14]. Ліву частину (13) отримаємо шляхом піднесення лівої і правої частин (14) у квадрат і розгляду оберненого до отриманого значення:

$$\frac{1}{cos^2\beta_{(m)}}=\frac{\sigma_1^{\,2m}(B)+\sigma_2^{\,2m}(B)+...+\sigma_l^{\,2m}(B)}{\sigma_1^{\,2m}(B)}=1+\left(\frac{\sigma_2(B)}{\sigma_1(B)}\right)^{2m}+...+\left(\frac{\sigma_l(B)}{\sigma_1(B)}\right)^{2m} \tag{15}$$

Кожен дріб в правій частині (15) задовольняє умові:

$$0\leq\frac{\sigma_i(B)}{\sigma_1(B)}<1,\ i=\overline{2,l}\,.$$

Враховуючи властивості показникової функції з основою, що менше одиниці, маємо при $p > m$:

$$\left(\frac{\sigma_i(B)}{\sigma_1(B)}\right)^{2p} < \left(\frac{\sigma_i(B)}{\sigma_1(B)}\right)^{2m}, i = \overline{2,l}, \quad (16)$$

З (16) випливає:

$$\frac{1}{cos^2\beta_{(p)}} < \frac{1}{cos^2\beta_{(m)}} \quad \Rightarrow \quad cos^2\beta_{(m)} < cos^2\beta_{(p)}.$$

З урахуванням того, що СНЧ будь-якої матриці є нечутливими до збурних дій, тобто кути $\beta_{(p)}, \beta_{(m)}$ - гострі, маємо:

$$\beta_{(p)} < \beta_{(m)},$$

що й потрібно було довести.

В [12], враховуючи актуальність оцінки чутливості для параметрів, що аналізуються в межах підходу, що розглядається, для виявлення порушення цілісності ЦЗ, було показано, що нормований вектор СНЧ $\bar{\sigma}$, що відповідає $l \times l$ – блоку B, будучи нечутливим, має більшу чутливість до збурних дій, ніж також нечутливий нормований вектор $\bar{\bar{\sigma}}$ СНЧ матриці BB^T ($B^T B$). Узагальненням цього є наступне твердження.

Твердження 4. Чутливість нормованого вектора $\bar{\sigma}^{(m)}$ є меншою за чутливість $\bar{\sigma}$ і спадає зі зростанням *m*.

Доказ. Доведення першої частини твердження аналогічне [12]. Нехай в результаті збурної дії блок B зазнав збурення ΔB, результатом чого є збурений блок $\overline{B}$ з СНЧ $\sigma_i(B + \Delta B), i = \overline{1,l}$. Для відповідних перетворених блоків (4) або (10) збурення відіб'ється на векторі $\bar{\sigma}^{(m)}$, який в результаті стане $\bar{\sigma}_{зб}^{(m)}$ і буде обчислюватися наступним чином:

$$\bar{\sigma}_{зб}^{(m)} = \frac{\left(\sigma_1^m(B + \Delta B), \ldots, \sigma_l^m(B + \Delta B)\right)}{\sqrt{\sigma_1^{2m}(B + \Delta B) + \ldots + \sigma_l^{2m}(B + \Delta B)}} \quad (17)$$

Оцінимо чутливість $\bar{\sigma}^{(m)}$ за допомогою кута повороту $\gamma_{(m)}$ між векторами $\bar{\sigma}^{(m)}$ і $\bar{\sigma}_{зб}^{(m)}$ (17):

$$cos(\gamma_{(m)}) = \frac{\left(\bar{\sigma}^{(m)}, \bar{\sigma}_{зб}^{(m)}\right)}{\left\|\bar{\sigma}^{(m)}\right\| \left\|\bar{\sigma}_{зб}^{(m)}\right\|} = \frac{\sigma_1^m(B)\sigma_1^m(B + \Delta B) + \ldots + \sigma_l^m(B)\sigma_l^m(B + \Delta B)}{\sqrt{\sigma_1^{2m}(B) + \ldots + \sigma_l^{2m}(B)}\sqrt{\sigma_1^{2m}(B + \Delta B) + \ldots + \sigma_l^{2m}(B + \Delta B)}}, \quad (18)$$

де $(\cdot,\cdot)$ – скалярний добуток векторів-аргументів.

Перетворену відповідно з (4) або (10) матрицю блоку *B* будемо позначати $(B)^{(m)}$, де *m* вказує на кількість використаних при перетворенні матриць-множників. Нехай $p > m$, тобто $p = m + c$, де $c > 0$, $cos(\gamma_{(p)})$ визначимо відповідно до (18). Тоді:

$$\frac{cos(\gamma_{(p)})}{cos(\gamma_{(m)})} = \frac{\left(\sigma_1^{m+c}(B)\sigma_1^{m+c}(B + \Delta B) + \ldots + \sigma_l^{m+c}(B)\sigma_l^{m+c}(B + \Delta B)\right)}{\sqrt{\sigma_1^{2(m+c)}(B) + \ldots + \sigma_l^{2(m+c)}(B)}\sqrt{\sigma_1^{2(m+c)}(B + \Delta B) + \ldots + \sigma_l^{2(m+c)}(B + \Delta B)}} \times$$
$$\times \frac{\sqrt{\sigma_1^{2m}(B) + \ldots + \sigma_l^{2m}(B)}\sqrt{\sigma_1^{2m}(B + \Delta B) + \ldots + \sigma_l^{2m}(B + \Delta B)}}{\left(\sigma_1^m(B)\sigma_1^m(B + \Delta B) + \ldots + \sigma_l^m(B)\sigma_l^m(B + \Delta B)\right)}.$$

Враховуючи співвідношення між матричною нормою Фробеніуса і складовими сингулярного спектру матриці [12], останнє співвідношення можна представити у вигляді:

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}=\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left\|(B)^{(m+c)}\right\|_F\left\|(B+\Delta B)^{(m+c)}\right\|_F}\times$$

$$\times\frac{\left\|(B)^{(m)}\right\|_F\left\|(B+\Delta B)^{(m)}\right\|_F}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)}. \qquad (19)$$

Враховуючи, що норма Фробеніуса добутку матриць не перевищує добутку норм множників [16], а також, що норми поданої і транспонованої матриці співпадають, з (19) отримуємо:

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}\geq\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left\|(B)^{(m)}\right\|_F\left\|(B+\Delta B)^{(m)}\right\|_F\left\|(B)^{(c)}\right\|_F\left\|(B+\Delta B)^{(c)}\right\|_F}\times$$

$$\times\frac{\left\|(B)^{(m)}\right\|_F\left\|(B+\Delta B)^{(m)}\right\|_F}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)}=$$

$$=\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\left\|(B)^{(c)}\right\|_F\left\|(B+\Delta B)^{(c)}\right\|_F}\geq \qquad (20)$$

$$=\frac{\left(\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)+\ldots+\sigma_l{}^{m+c}(B)\sigma_l{}^{m+c}(B+\Delta B)\right)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\|B\|_F^c\|B+\Delta B\|_F^c}\geq$$

$$\geq\frac{\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\|B\|_F^c\|B+\Delta B\|_F^c}.$$

Враховуючи (12), визначення спектральної матричної норми [16], порівнянність спектральної матричної норми і норми Фробеніуса для блоку оригінального ЦЗ [12], з (20) отримуємо:

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}\geq$$

$$\geq\frac{\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)}{\left(\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)+\ldots+\sigma_l{}^{m}(B)\sigma_l{}^{m}(B+\Delta B)\right)\|B\|_F^c\|B+\Delta B\|_F^c}\approx\frac{\sigma_1{}^{m+c}(B)\sigma_1{}^{m+c}(B+\Delta B)}{\sigma_1{}^{m}(B)\sigma_1{}^{m}(B+\Delta B)\|B\|_F^c\|B+\Delta B\|_F^c}=$$

$$=\frac{\|B\|_2^{m+c}\|B+\Delta B\|_2^{m+c}}{\|B\|_2^{m}\|B+\Delta B\|_2^{m}\|B\|_F^c\|B+\Delta B\|_F^c},$$

тобто

$$\frac{cos\left(\gamma_{(p)}\right)}{cos\left(\gamma_{(m)}\right)}\geq 1,$$

що й потрібно було довести.

Оскільки при перетвореннях (4), (10) СНВ перетворених матриць відповідають СНВ блоку B, то їх реакція на збурюючу дію ΔB в межах B і перетворених матриць буде визначатися однаково.

З доведених вище тверджень випливає істинність

Твердження 5. Для блоку B зображення пара векторів $u_1,\overline{\sigma}^{(m)}$ є більш стійкою до збурних дій, ніж пара $u_1,\overline{\sigma}$ у тому розумінні, що в результаті

збурюючої дії величина кута між $u_1, \overline{\sigma}^{(m)}$ збуриться менше, ніж між $u_1, \overline{\sigma}$, при цьому ця стійкість буде зростати разом зі зростанням m.

З врахуванням вищенаведеного має місце наступна теорема.

Теорема. Співвідношення

$$\angle\left(u_1, \overline{\sigma}^{(m)}\right) \approx \angle\left(v_1, \overline{\sigma}^{(m)}\right) \approx \angle\left(n^O, e_1\right), \tag{21}$$

виконується для більшості блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, при цьому рівність в (21) має місце для більшої кількості блоків більшої кількості оригінальних ЦЗ при $m > 2$, ніж при $m = 2$.

Таким чином, з точки зору отриманих теоретичних результатів, використання перетворень (4), (10) для $k > 1$ очікувано повинно дати підвищення ефективності методів експертизи цілісності ЦЗ, що базуються на підході, який розглядається в роботі, в частині підтвердження збереження зображеннями цілісності.

Для практичної перевірки висновку теореми був проведений обчислювальний експеримент, в якому було задіяно 1000 ЦЗ розміром 400×400 пікселів: 500 ЦЗ з бази NRCS [17], 500 ЦЗ з бази img_Nikon_D70s [18].

Ілюстрація, яка має типовий характер, і підтверджує висновок теореми, наведена на рис.2 для ЦЗ (рис.1), $l = 4$.

Рис.1. Тестове ЦЗ

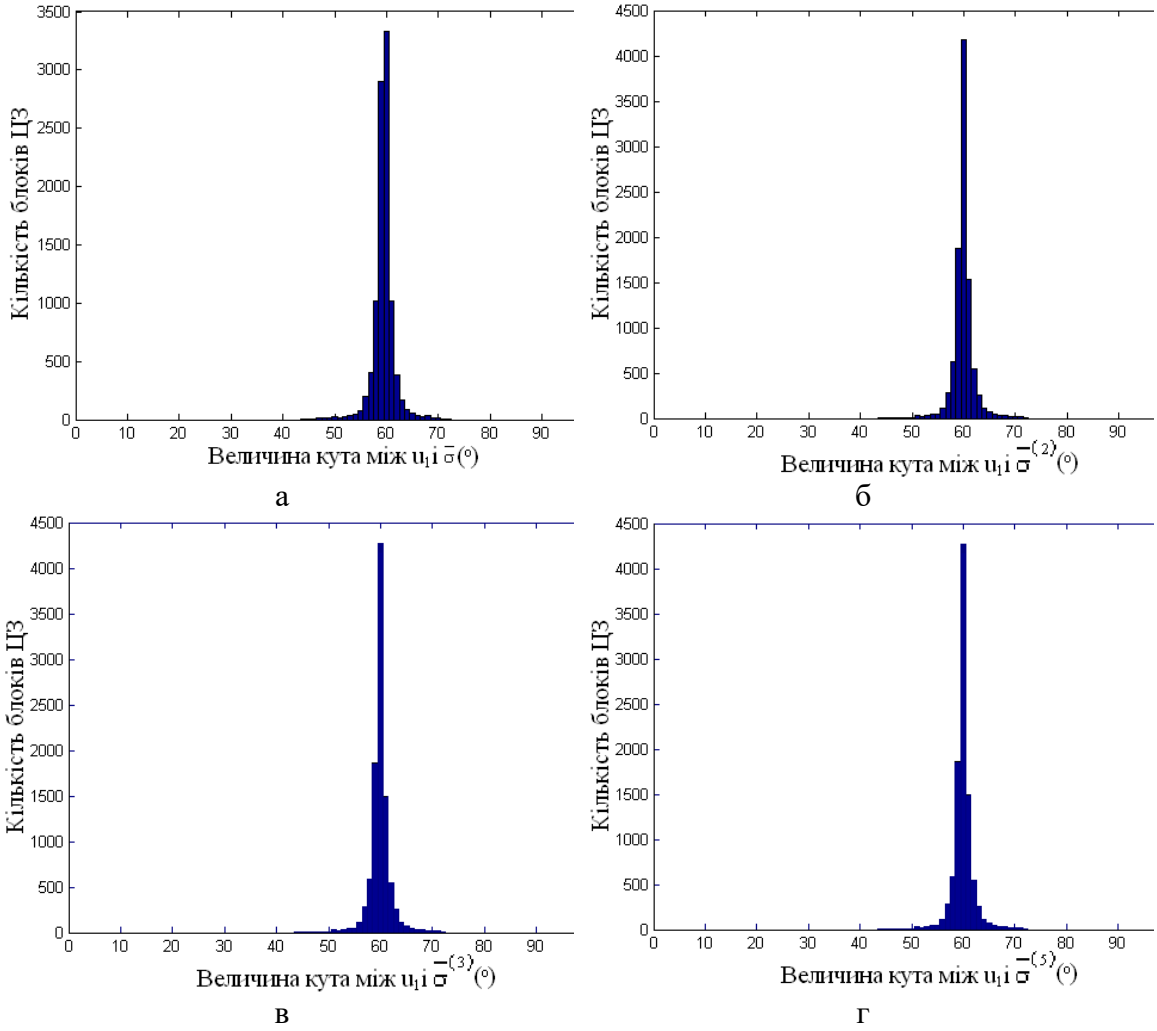

Рис.2. Ілюстрація виконання співвідношення (21) для оригінального ЦЗ при різних значеннях m: а – аналізуються вектори $u_1, \bar{\sigma}$; б - вектори $u_1, \bar{\sigma}^{(2)}$; в - вектори $u_1, \bar{\sigma}^{(3)}$; г - вектори $u_1, \bar{\sigma}^{(5)}$

Як видно з рис.2(б,в,г), характер змін гістограми хоча і відповідає теоремі (збільшення значення в моді, яка співпадає з $\angle\left(n^O, e_1\right)$), але кількісно ці зміни при $m > 2$ є незначними, аж до непомітних (порівн. рис.2(в), рис.2(г)). Це має пояснення. Дійсно, починаючи з деякого значення $m > 2$, відокремленість максимального СНЧ блоку $(B)^{(m)}$ стає настільки великою, що при нормуванні відповідного вектору СНЧ отримується вектор e_1, і подальше підвищення ступеня m тут вже нічого не змінює для ступеня близькості нормованого вектора СНЧ і e_1. Найбільший ефект тут досягається при переході від аналізу векторів $u_1, \bar{\sigma}$ до векторів $u_1, \bar{\sigma}^{(2)}$. Але, як показує обчислювальний експеримент, для підвищення ефективності при встановленні оригінальності ЦЗ (зниженні помилок 2-го роду для відповідних експертних методів) має сенс використовувати $m = 3$.

Підвищення стійкості пари векторів $u_1, \bar{\sigma}^{(m)}$ разом зі зростанням m має і негативні наслідки в світлі проблеми, що розглядається. Дійсно, зниження чутливості до збурних дій сприяє підвищенню ефективності виявлення ЦЗ, цілісність яких порушена не була, але це зниження дещо ускладнює виявлення змінених ЦЗ. Дійсно, чим стійкіша пара $u_1, \bar{\sigma}^{(m)}$, тим менше вона «реагує» на будь-

яку збурну дію, утруднюючи пошук властивостей відповідних гістограм, які і вказують на це порушення, що знайшло своє підтвердження на практиці в результаті обчислювального експерименту, в якому були задіяні 1000 ЦЗ, описаних вище. Ілюстрація цьому наведена на рис.3 для того ж ЦЗ (рис.1), яке використовувалося в оригінальному вигляді на рис.2. В якості збурної дії тут використовувалось накладання гауссівського шуму з нульовим математичним очікуванням і D=0.005.

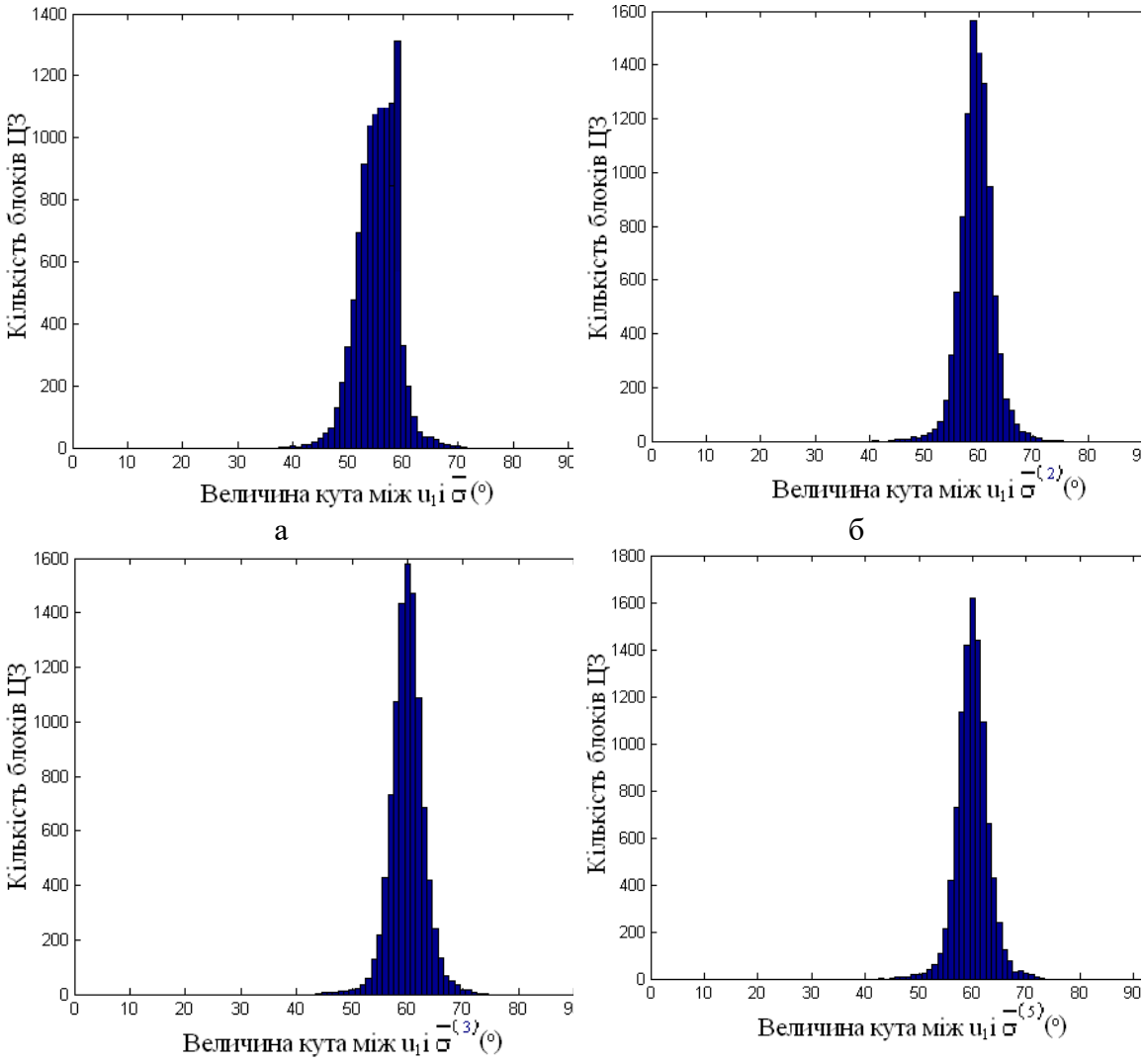

Рис.3. Гістограми значень кутів (21) для ЦЗ, цілісність якого порушена: а – аналізуються вектори $u_1, \bar{\sigma}$; б - вектори $u_1, \bar{\sigma}^{(2)}$; в - вектори $u_1, \bar{\sigma}^{(3)}$; г - вектори $u_1, \bar{\sigma}^{(5)}$

Найзначнішою тут є реакція пари векторів $u_1, \bar{\sigma}$ і $u_1, \bar{\sigma}^{(2)}$, яка приводить до зміни положення моди гістограми в результаті збурення ЦЗ, а при $m > 2$, мода не змінює своє положення відносно того, яким воно було для оригінального ЦЗ. І хоча гістограми оригінального і збуреного ЦЗ навіть при співпадінні моди значно відрізняються (порівн. рис.2(в) і 3(в); рис.2(г) і 3(г)): значення гістограми в моді менше для збуреного ЦЗ майже в 3 рази, велика кількість блоків збуреного ЦЗ має кут між $u_1, \bar{\sigma}^{(m)}$, $m > 2$, близький до моди, що є очікуваним і випливає з [11-14], але при відсутності гістограми відповідного оригінального ЦЗ, що є стандартною

ситуацією на практиці при проведенні експертизи цілісності, встановити її порушення буде тут складніше, ніж у випадку $m = 2$. Підвищення стійкості пари $u_1, \overline{\sigma}^{(m)}$, що має місце зі зростанням *m*, є очевидним і у випадку ЦЗ, цілісність якого порушена: мода не тільки не зсувається з місця $\angle\left(n^O, e_1\right)$, але й значення гістограми в моді зростає (див.рис.3(в, г)).

Таким чином, на практиці не має сенсу підвищувати значення *m* більше двох, що, підвищуючи обчислювальну складність процесу експертизи ЦЗ, принципово не зможе покращити ефективність експертних методів, заснованих на розглянутому підході, зменшуючи кількість помилок другого роду при очікуваному збільшенні кількості помилок першого роду.

Висновки

В роботі проаналізовані різноманітні перетворення матриці блока ЦЗ з метою їх використання для підвищення ефективності експертизи цілісності ЦЗ, що базується на аналізі властивостей СНЧ і СНВ блоків матриці контенту, отриманих шляхом її стандартної розбивки. Встановлено, що для підвищення ефективності підтвердження збереження цілісності ЦЗ має сенс використовувати перетворення виду (4) при *m*=2, виду (10) при *m*=3, але з урахуванням пріоритетності виявлення саме порушення цілісності в загальному випадку перевагу треба віддати перетворенню (4) з *m*=2.

Список літератури

1. Пирцхалава Л.Г. Информационное противоборство в современных условиях. К.: ЦП Компринт, 2019. 226 с.
2. Appari A., Johnson M.E. Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*. 2010. 6(4). P. 279–314
3. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Boston: Springer, 2012. 100 p.
4. Mazurczyk W. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures /. Hoboken: Wiley, 2016. 296 p.
5. Heatherly R., Kantarcioglu M., Thuraisingham B. Preventing private information inference attacks on social networks. *IEEE Transactions on Knowledge and Data Engineering*. 2013. 25(8). P. 1849–1862.
6. Задірака, В.К. Сучасні методи розв'язання задач інформаційної безпеки. *Вісник НАН України*. 2014. 5. С. 65–69.
7. Milov O. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. *Восточно-Европейский журнал передовых технологий*. 2019. 2(9). С. 56–66.
8. Uliyan D.M. Image region duplication forgery detection based on angular radial partitioning and Harris key-points. *Symmetry*. 2016. 8(7). 62.
9. 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.
10. Кобозева, А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. *Праці Одеського політехнічного університету*. 2014. 2. С. 136–146.
11. Бобок И.И. Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров. *Інформатика та математичні методи в моделюванні*. 2017. 7(3). С. 170–177.

12. Бобок І.І. Дослідження властивостей формальних параметрів цифрового зображення в умовах порушення його цілісності. *Сучасна спеціальна техніка*. 2017. 4(51). С. 6–16.;
13. Бобок І.І Розвиток загального підходу до проблеми виявлення порушень цілісності цифрових зображень. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2017. 2(34). С. 78–88.
14. Бобок І.І. Розвиток теоретичних основ підходу до проблеми виявлення порушень цілісності цифрового зображення. *Перспективні напрями захисту інформації*: матеріали V Всеукр. наук.-практ. конф. Одеса, 2019. С. 17–19
15. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
16. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
17. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
18. Gloe T., Böhme R. The “Dresden Image Database” for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC ’10)*. New York, 2010. P. 1585–1591.

INVESTIGATION OF THE PARAMETERS OF THE CONVERTED BLOCKS OF A DIGITAL IMAGE TO DETECT VIOLATIONS OF ITS INTEGRITY

I.I. Bobok

National Odesa Polytechnic University, ave. Shevchenko, 1, Odesa, 65044, Ukraine
onu_metal@ukr.net

The problem of detecting the integrity violations of information content is one of the main problems of modern information security. Unauthorized modified information content when used for non-entertainment purposes can lead to critically negative consequences for individuals, enterprises, banks, firms, and catastrophic consequences for humanity as a whole if cyber-attacks are directed at the military, energy, chemical industry, etc. The world scientific community pays a lot of attention to the problem of detecting the integrity violations of information content, in particular digital images considered in the work, but this problem does not have a final solution, the task of improving approaches and methods of examination of the integrity of digital content will remain relevant. The aim of the work is to investigate the possibilities of improving the existing approach to detecting unauthorized changes of digital images, based on the analysis of singular values and singular vectors of the blocks of the corresponding matrix, by studying the properties of the blocks obtained using various transformations that differ from those proposed earlier. The properties of the blocks obtained by general symmetrization, as well as by the proposed transformations, which result in asymmetric matrices that can use an arbitrary number of m matrix-multipliers, are investigated. It has been established that to increase the effectiveness of confirming the integrity of the image, it makes sense to use symmetric blocks at m=2, non-symmetrized blocks at m=3, but taking into account the priority of detecting integrity violations, in the general case preference should be given to the symmetrization transformation with m=2.

Keywords: digital image integrity, integrity violation, singular value, singular vector, sensitivity to disturbances