УДК 004.056.5

д.т.н., проф. **Кобозєва А.А.** (ОНПУ)
д.т.н., проф. **Маєвський Д.А.** (ОНПУ)
Кирилюк В.О. (ОНПУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-08

МЕТОД ВИЯВЛЕННЯ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ, ЗАСНОВАНИЙ НА СПЕКТРАЛЬНОМУ РОЗКЛАДАННІ СИМЕТРИЗОВАНОЇ МАТРИЦІ БЛОКУ

В роботі розглядається важлива науково-практична задача підвищення ефективності виявлення порушень цілісності інформації, зокрема цифрових зображень, що є її поширеним представленням, яка стає сьогодні одною з основних для фахівців в області інформаційної та кібербезпеки. Невиявлені своєчасно несанкціоновані зміни інформації можуть привести до негативних, катастрофічних наслідків як для окремих людей, підприємств, банків, фірм, так і для людства в цілому, коли йдеться про інформацію, що становить державну таємницю, містить дані зі сфери військової галузі, атомної енергетики, хімічної промисловості тощо, що визначає актуальність задачі, яка розглядається. Основним результатом роботи є удосконалений універсальний метод виявлення порушення цілісності цифрового зображення, готовий до практичної реалізації, теоретичний базис якого заснований на аналізі власних значень та власних векторів симетричних блоків матриці зображення, що ставляться у відповідність оригінальним блокам. В роботі обгрунтований спосіб симетризації матриці блоку, що дозволяє значно (більше, чим на 23%) скоротити обчислювальні і, як наслідок, часові витрати на експертизу зображення в порівнянні з часовими витратами методу-прототипу. Доведено, що для більшості отриманих симетричних блоків, що ставляться у відповідність блокам оригінального ЦЗ, кут між власним вектором, що відповідає максимальному власному значенню блока, і нормованим вектором модулів власних значень дорівнює певному значенню, яке не залежить від конкретики оригінального зображення, але є чутливим до його змін, що дало можливість забезпечити універсальність методу та підвищити його ефективність у сенсі точності виявлення порушення цілісності зображення більше, ніж на 5%, в порівнянні з аналогом. Значимість отриманих результатів полягає в забезпеченні за рахунок використання запропонованого методу підвищення ефективності процесу виявлення порушень цілісності зображення за критеріями обчислювальних (часових) витрат на експертизу одного зображення та точності виявлення.

***Ключові слова**: цифрове зображення, порушення цілісності, власний вектор, власне значення.*

Вступ. Стрімкий розвиток інформаційних технологій, проникнення їх у всі сфери людської діяльності привів сучасне суспільство до стану, при якому несанкціоновані зміни інформації – порушення її цілісності можуть привести до негативних наслідків як для окремих людей, підприємств, банків, фірм, так і до катастроф для людства в цілому, якщо несанкціоновані зміни відбудуться з інформацією, що становить державну таємницю, містить дані зі сфери військової галузі, атомної енергетики, хімічної промисловості тощо, що може поставити під загрозу життя людей в усьому світі [1] і що є критично актуальним для нашої держави сьогодні, під час повномасштабного вторгнення Росії в Україну.

Питання виявлення порушень цілісності інформації – одного з критеріїв її захищеності, зокрема цифрових зображень (ЦЗ), що є її поширеним представленням, стає сьогодні одним з основних для фахівців в області інформаційної та кібербезпеки [2,3]. Ці порушення можуть проводитися різними способами, мати різні цілі. Так організація прихованого

(стеганографічного) каналу зв'язку, де порушення цілісності контейнера є результатом вбудови в нього додаткової інформації, може сприяти безпосередньо витоку секретної інформації, привести до матеріального, репутаційного збитку підприємств, фірм, банків, до наслідків державного масштабу [4]; застосування засобів графічних редакторів (Adobe Photoshop, Gimp та ін.) дозволяє, навіть не маючи спеціальної кваліфікації, обробляти, змінювати ЦЗ, цифрові відео, результатом чого може стати, зокрема усунення зі сцени ЦЗ (кадрів відео) окремих предметів, персонажів чи їх штучне додавання, що кардинально змінить зміст цифрового контенту та наслідки від його використання [5], може виявитися критичним при застосуванні таких контентів в судових справах, засобах масової інформації тощо. Тільки своєчасне виявлення неоригінальності цифрового контенту дозволить тут уникнути негативних наслідків, що говорить про актуальність і важливість розробки, модифікації, удосконалення відповідних методів, спрямованих на виявлення порушення цілісності інформаційного контенту, зокрема ЦЗ.

Аналіз останніх досліджень і публікацій. Методи виявлення порушення цілісності ЦЗ розподіляються на дві великі групи: активні і пасивні (або «сліпі») [6,7]. Активні методи, більшість із яких використовують електронний цифровий підпис або цифрові водяні знаки, потребують інформацію про оригінальне ЦЗ, на відміну від пасивних, для яких така інформація не потрібна. На сьогоднішній день саме пасивні експертні методи займають провідні позиції для розв'язку задачі, що розглядається [7-9], хоча організація «сліпого» детектування результатів порушення цілісності ЦЗ є більш складною. Всі пасивні методи в свою чергу, залежно від інформації, що є в наявності у експерта, можна розподілити на спрямовані (налаштовані на конкретні збурні дії, які враховують особливості, властивості тих збурень, що є результатом таких дій) та універсальні (налаштовані на виявлення наявності відмін досліджуванного контента від оригінального незалежно від того, яким чином ці зміни були отримані). Спрямовані методи, як правило, є більш ефективними при виявленні тої дії, на яку вони налаштовані, ніж універсальні в тих самих умовах застосування. Але, враховуючи те, що на практиці обізнаність експерта про можливі збурні дії не завжди присутня, наявний у експерта арсенал програмних засобів є обмеженим та принципово не може (у випадку спрямованих методів) забезпечити «готовність» до всіх збурних дій, надзвичайно актуальним на сьогодні є наявність, розробка, удосконалення саме універсальних методів для розв'язку задачі, що розглядається. І хоча розробки в цьому напрямку ведуться [10,11], при цьому найчастіше – в межах стеганоаналізу [12,13], на сьогоднішній день універсальні методи виявлення порушення цілісності ЦЗ майже відсутні, а зусилля вчених найчастіше спрямовані на виявлення результатів конкретних збурних дій: зміни яскравості [14], розмиття ЦЗ чи його частини [15], накладання шуму [16], результатів стеганоперетворення конкретними стеганоалгоритмами [17,18] тощо. Математичний базис таких методів формується з врахуванням особливостей, які вносять саме ці конкретні збурні дії в параметри оригінального ЦЗ. Так в [14] знайдене формальне представлення результату корекції яскравості ЦЗ у вигляді корекції максимального сингулярного числа σ_1 його матриці яскравості Y, яке і використане в відповідному експертному методі. В [19] запропонований метод виявлення результатів штучного підвищення різкості в ЦЗ, розглянутий конкретний фільтр, що використовується для цієї операції в графічному редакторі AdobePhotoshop – «Інтелектуальна різкість». Для відокремлення ЦЗ, що піддалися обробці таким фільтром, від таких, що не піддалися, використовується оцінка відношення кількості близьких пар кольорів до загальної кількості пар кольорів, яка специфічно змінюється при застосуванні згаданого фільтра, для якої імпірічно визначене порогове значення. В [17,18.] запропоновані стеганоаналітичні методи, спрямовані на виявлення результатів стеганоперетворення LSB-методом. Ці методи не тільки налаштовані на конкретний стеганографічний метод, а ще й накладають обмеження на

величину пропускної спроможності прихованого каналу зв'язку, що піддається експертизі. Існує ціла низка методів, які застосовуються для аналізу ЦЗ у форматі Jpeg, заснованих на виявленні «ефекту подвійного квантування», що виникає в гістограмах частотних коефіцієнтів зображення при первісному та повторному його збереженні в Jpeg, які мають значне поширення в силу широкого використання цього формату сьогодні для збереження ЦЗ [9,20], але очевидно, що «форматоорієнтованість» значно обмежує область застосування таких методів для експертизи цілісності і не дає можливості віднести їх до групи універсальних.

Одним з невеликої кількості існуючих універсальних пасивних методів виявлення порушення цілісності ЦЗ є метод, запропонований в [11]. Основою методу є доведена для більшості $l \times l$-блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, рівність:

$$\angle\left(u_1, \bar{\sigma}\right) \approx \angle\left(v_1, \bar{\sigma}\right) \approx \angle\left(n^{\circ}, e_1\right), \qquad (1)$$

де u_1, v_1 – ортонормовані сингулярні вектори (СНВ) блоку, що відповідають найбільшому сингулярному числу σ_1; $\bar{\sigma} = \sigma / \|\sigma\|$, де $\sigma = (\sigma_1, \sigma_2, ..., \sigma_i)^T$, $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_i \geq 0$ – сингулярні числа (СНЧ) блоку; $n^{\circ} = \left(1/\sqrt{l}, 1/\sqrt{l}, ..., 1/\sqrt{l}\right)^T \in R^l$ – *n*-оптимальний вектор простору R^l, $\angle\left(u_1, \bar{\sigma}\right)$, $\angle\left(v_1, \bar{\sigma}\right)$, $\angle\left(n^{\circ}, e_1\right)$ – величини кутів між векторами u_1 і $\bar{\sigma}$, v_1 і $\bar{\sigma}$, n° і вектором стандартного базису $e_1 = (1, 0, ..., 0)$ простору R^l, що відповідає додатному напряму осі Ox_1, відповідно. Значимою перевагою цього методу є те, що він залишається ефективним, незалежно від конкретики та сили збурної дії, в результаті якої відбувається порушення цілісності ЦЗ, від формату зображення. Але орієнтованість його на аналіз властивостей СНЧ, СНВ блоків, для отримання яких використовується їх нормальні сингулярні розкладання, які є достатньо «дорогими» в обчислювальному сенсі, робить актуальним питання його удосконалення при збереженні всіх переваг, як і метода, запропонованого в [21].

Таким чином, на основі проведеного аналізу наукових джерел встановлено, що проблема виявлення порушень цілісності ЦЗ не є вирішеною остаточно. Абсолютна більшість існуючих пасивних методів, що займають провідні позиції для розв'язку задачі, що розглядається, мають значні недоліки, серед яких: орієнтованість здебільшого на конкретну збурну дію, на формат ЦЗ, величину збурення, що зазнає оригінальний контент в результаті збурної дії, значні часові витрати, залишаючи *актуальною* задачу підвищення ефективності процесу виявлення порушень цілісності ЦЗ.

Мета роботи та задачі дослідження. *Метою* роботи є підвищення ефективності виявлення порушень цілісності ЦЗ шляхом удосконалення універсального методу, запропонованого в [11].

Як показники ефективності далі розглядаються: обчислювальні (часові) витрати на експертизу одного ЦЗ; точність виявлення порушення цілісності [22] (*accuracy* (*ACC*)), яка визначається відповідно до формули:

$$ACC = (TP + TN)/(TP + FN + TN + FP), \qquad (2)$$

де *TP* (*True Positive*) – число правильно виявлених ЦЗ, цілісність яких була порушена; *TN* (*True Negative*) – число правильно виявлених оригінальних ЦЗ; *FP* (*False Positive*) – число оригінальних ЦЗ, помилково прийнятих за такі, цілісність яких була порушена; *FN* (*False Negative*) – число ЦЗ, цілісність яких була порушена, помилково визнаних оригінальними.

Для досягнення поставленої мети в роботі розв'язуються наступні *задачі*:

1. Обгрунтувати спосіб симетризації матриці блоку ЦЗ, що дасть можливість заміни формальних параметрів блоку (СНЧ, СНВ), що використовуються в процесі експертизи в [11], на власні вектори і власні значення, отримання яких є менш обчислювально затратним;

2. Обгрунтувати математично можливість використання симетризованих блоків матриці ЦЗ для експертизи його цілісності;

3. Розробити удосконалення методу [11] та його алгоритмічну реалізацію;

4. Провести оцінку ефективності запропонованої алгоритмічної реалізації.

Основний матеріал дослідження. Нехай формальним представлення ЦЗ є $n \times n$-матриця F. У випадку кольорового зображення ця матриця може відповідати будь-якій кольоровій складовій (схема RGB) чи є матрицею яскравості (схема YUV). Матриця F стандартним чином [23] розбивається на непересічні $l \times l$-блоки, довільний з яких позначимо A. Для матриці A, у якої відсутні кратні СНЧ, маємо єдине нормальне сингулярне розкладання [24]:

$$A = U\Sigma V^T = \sum_{i=1}^{l} \sigma_i u_i v_i^T, \quad (3)$$

де U, V – ортогональні $l \times l$-матриці, стовпці яких u_i, v_i, $i = \overline{1,l}$, є лівими і правими СНВ A відповідно, при цьому ліві СНВ додатково є лексикографічно додатними; $\Sigma = diag(\sigma_1,..., \sigma_l), \sigma_1 \geq ... \geq \sigma_l \geq 0$ – СНЧ A. Права частина (3) представляє сингулярне розкладання A у формі зовнішніх добутків [25].

Якщо матриця A є симетричною, то всі її власні значення (ВЗ) є дійсними, при цьому для неї можливо побудувати єдине нормальне спектральне розкладання у випадку відсутності ВЗ з однаковими абсолютними значеннями:

$$A = W\Lambda W^T = \sum_{i=1}^{l} \lambda_i w_i w_i^T, \quad (4)$$

де W – ортогональна $l \times l$-матриця, стовпці якої w_i, $i = \overline{1,l}$, є лексикографічно додатними власними векторами (ВВ) A, $\Lambda = diag(\lambda_1,..., \lambda_l)$, $\lambda_1,..., \lambda_l$ – ВЗ A. Права частина (4) представляє спектральне розкладання A у формі зовнішніх добутків [25].

Спектральне і сингулярне розкладання симетричної матриці пов'язані між собою [25]. При цьому очевидним є те, що обчислювальна складність процесу побудови сингулярного розкладання A, яке передбачає визначення елементів матриць U, V і діагональної матриці Σ і оцінюється як $O(l^3)$, приблизно вдвічі більше, ніж спектрального, де передбачається обчислення елементів лише матриці W і діагональної матриці Λ (таке ж саме співвідношення буде мати місце і для запитів до пам'яті). Таким чином, одним з шляхів удосконалення методу з [11], що очікувано сприятиме зменшенню часових витрат на експертизу ЦЗ, є побудова експертизи не на аналізі СНЧ і СНВ реальних блоків, а на аналізі ВЗ і ВВ для симетричних матриць блоків (якщо цю симетричність можливо буде забезпечити без втрати точності виявлення порушення цілісності *ACC* та без виникнення обмежень на застосування відповідного методу). Дійсно, хоча обчислювальна складність будь-якого блокового методу, яким є і метод [11], визначається кількістю $l \times l$-блоків ЦЗ і для $n \times n$-матриці F становить $C\left\lceil \frac{n}{l} \right\rceil \times \left\lceil \frac{n}{l} \right\rceil = O(n^2)$, де C не залежить від n, незалежно від того, яка кількість операцій використовується для роботи з одним блоком, але кількість операцій обробки блоку

відіб'ється на коефіцієнті при n^2 і при застосуванні спектрального розкладання для матриці блоку цей коефіцієнт очевидно буде менше, чим при використанні сингулярного розкладання. Але в ЦЗ блок, як правило, не є симетричним. Розглянемо декілька можливих способів отримання симетричного виду блоку B, що буде ставитися у співвідношення реальному блоку A ЦЗ при його експертизі:

$$A \quad \rightarrow \quad B = A^T A, \tag{5}$$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{21} & a_{22} & \dots & a_{2l} \\ \dots\dots\dots & \dots\dots\dots & & \\ a_{l1} & a_{l2} & \dots & a_{ll} \end{pmatrix} \quad \rightarrow \quad B = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{l1} \\ a_{21} & a_{22} & \dots & a_{l2} \\ \dots\dots\dots & \dots\dots\dots & & \\ a_{l1} & a_{l2} & \dots & a_{ll} \end{pmatrix} \quad \vee \quad B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{12} & a_{22} & \dots & a_{2l} \\ \dots\dots\dots & \dots\dots\dots & & \\ a_{1l} & a_{2l} & \dots & a_{ll} \end{pmatrix}, \tag{6}$$

$$A \quad \rightarrow \quad B = \frac{A + A^T}{2}. \tag{7}$$

Обчислювальна складність симетризації (5) визначається як $O\left(l^3\right)$, для (7) – $O\left(l^2\right)$. Використання одної з матриць B, що визначаються (6), взагалі не вимагає проведення жодної арифметичної операції для перерахування елементів B відносно A, а може бути сформована лише за $O\left(l^2\right)$ операцій присвоювання, виконання яких вимагає меньшого часу, ніж будь-яка арифметична операція. На перший погляд, з точки зору часових витрат, перевагу треба віддати способу (6), але для кожного з варіантів (6) матриця B несе в собі інформацію лише про нижній/верхній трикутник оригінальної матриці A, при цьому інформація про верхній/нижній трикутник губиться, а загалом губиться майже половина інформації про досліджуване ЦЗ, що є неприпустимим з урахуванням специфіки задачі, що розглядається в роботі. Передбаченим результатом цього, який підтверджено практично, є, на фоні зменшення часу експертизи, значне зменшення ефективності експертизи (*ACC*) в порівнянні з [11], що, з урахуванням вищенаведеного, робить пріоритетним спосіб (7) для симетризації блоку, який хоча дещо і спотворює інформацію про реальні значення матриці A, але зберігає її в цілому про блок A.

Враховуючи форму (3) сингулярного розкладання, з (7) для симетричної матриці B маємо:

$$B = \frac{A + A^T}{2} = \frac{U\Sigma V^T + V\Sigma U^T}{2} = \frac{1}{2}\left(\sum_{i=1}^{l} \sigma_i u_i v_i^T + \sum_{i=1}^{l} \sigma_i v_i u_i^T \right) = \frac{1}{2} \sum_{i=1}^{i} \sigma_i \left(u_i v_i^T + v_i u_i^T \right) =$$

$$= \frac{1}{2}\left(\sigma_1 \left(u_1 v_1^T + v_1 u_1^T \right) + \sum_{i=2}^{l} \sigma_i \left(u_i v_i^T + v_i u_i^T \right) \right). \tag{8}$$

Як доведено в [26], для СНВ u_1, v_1 блоку оригінального ЦЗ, що відповідають максимальному СНЧ σ_1:

$$u_1 \approx n^\circ, \quad v_1 \approx n^\circ. \tag{9}$$

Підставимо (9) в (8):

$$B = \frac{1}{2}\left(\sigma_1 \left(n^{\circ} \left(n^{\circ}\right)^T + n^{\circ}\left(n^{\circ}\right)^T \right) + \sum_{i=2}^{l} \sigma_i \left(u_i v_i^T + v_i u_i^T \right) \right) = \sigma_1 n^{\circ}\left(n^{\circ}\right)^T + \frac{1}{2}\sum_{i=2}^{l} \sigma_i \left(u_i v_i^T + v_i u_i^T \right). \quad (10)$$

Для симетричної матриці B існує певний зв'язок між її сингулярним і спектральним розкладанням [25]. Якщо у відповідності до (4) позначити спектральне розкладання B: $B = \overline{U}\,\overline{\Lambda}\,\overline{U}^T$ ($\overline{\Lambda} = diag\left(\bar{\lambda}_1, \bar{\lambda}_2, ..., \bar{\lambda}_l\right)$ – матриця ВЗ, $\overline{U} = \left(\bar{u}_1, \bar{u}_2, ..., \bar{u}_l\right)$ – ортогональна матриця ВВ), то сингулярне розкладання для B виглядає: $B = \overline{U}\,\overline{\Sigma}\,\overline{V}^T$ ($\overline{\Sigma} = diag\left(\bar{\sigma}_1, \bar{\sigma}_2, ..., \bar{\sigma}_n\right)$ – матриця СНЧ, $\overline{V} = \left(\bar{v}_1, \bar{v}_2, ..., \bar{v}_l\right)$ – ортогональна матриця правих СНВ), де

$$\bar{\sigma}_i = \left|\bar{\lambda}_i\right|, \; \bar{v}_i = sign\left(\bar{\lambda}_i\right)\bar{u}_i. \quad (11)$$

З урахуванням (9) для B при отриманні її сингулярного розкладання: $\bar{u}_1 \approx n^{\circ}$, $\bar{v}_1 \approx n^{\circ}$. Це означає, що для першого власного вектора B, що отримується при спектральному розкладанні B і відповідає максимальному за модулем ВЗ, яке за теоремою Фробеніуса [27] є додатним: $\bar{u}_1 \approx n^{\circ}$.

Якщо б для B будувалось спектральне розкладання у формі зовнішніх добутків, то ми б отримали:

$$B = \sum_{i=1}^{l} \bar{\lambda}_i \bar{u}_i \left(\bar{u}_i\right)^T = \bar{\lambda}_1 \bar{u}_1 \left(\bar{u}_1\right)^T + \sum_{i=2}^{l} \bar{\lambda}_i \bar{u}_i \left(\bar{u}_i\right)^T = \bar{\lambda}_1 n^{\circ}\left(n^{\circ}\right)^T + \sum_{i=2}^{n} \bar{\lambda}_i \bar{u}_i \left(\bar{u}_i\right)^T. \quad (12)$$

А якщо б для B будувалось сингулярне розкладання у формі зовнішніх добутків, воно б мало вигляд:

$$B = \sum_{i=1}^{l} \bar{\sigma}_i \bar{u}_i \left(\bar{v}_i\right)^T = \bar{\sigma}_1 \bar{u}_1 \left(\bar{v}_1\right)^T + \sum_{i=2}^{l} \bar{\sigma}_i \bar{u}_i \left(\bar{v}_i\right)^T = \bar{\sigma}_1 n^{\circ}\left(n^{\circ}\right)^T + \sum_{i=2}^{l} \bar{\sigma}_i \bar{u}_i \left(\bar{v}_i\right)^T. \quad (13)$$

Враховуючи ортогональність ВВ, СНВ B, можна стверджувати, що серед власних векторів, як і серед лівих і правих СНВ B є тільки по одному, що дорівнюють n°. Це вектори, що відповідають найбільшому ВЗ/найбільшому СНЧ. Таким чином, перший доданок в правій частині (10) можна розглядати, як добуток першого (максимального) власного значення на відповідний власний вектор. Порівнюючи праві частини (10), (12) і (13), враховуючи (11), маємо:

$$\bar{\lambda}_1 = \bar{\sigma}_1 = \sigma_1. \quad (14)$$

Основою співвідношення (1) разом з (9) було в [26] співвідношення $\bar{\sigma} \approx e_1$, отримане з урахуванням того, що для блоків ЦЗ максимальне СНЧ є набагато більшим за всі інші СНЧ. Операція (7), усереднюючі значення яскравості пікселєй, розмиває блок, зменшуючи його високочастотну складову. Для СНЧ, враховуючи зв'язок між сингулярними тройками (блоку) матриці ЦЗ та її частотними коефіцієнтами, що полягає в тому, що сингулярні трійки, що відповідають максимальним/мінімальним/середнім СНЧ несуть в собі інформацію, головним чином, про низькочастотну/високочастотну/середньочастотну складову сигналу, це приводить до сукупного зменшення найменших і, можливо, середніх значень СНЧ, що, враховуючи (11), (14), приведе до того, що $\bar{\lambda}_1$ буде мати більшу абсолютну відокремленість

$$gap_{abs}(1,B) = \min_{i\neq 1}\left\|\left|\bar{\lambda}_1\right| - \left|\bar{\lambda}_i\right|\right\|, \tag{15}$$

ніж відокремленість $svdgap(1,A) = \min_{i\neq 1}\left|\sigma_1 - \sigma_i\right|$ СНЧ σ_1 в A. Наслідком цього, в свою чергу, буде те, що нормований вектор модулів власних значень B

$$\bar{\lambda} = \frac{\lambda}{\|\lambda\|}, \tag{16}$$

де $\lambda = \left(\bar{\lambda}_1, \left|\bar{\lambda}_2\right|, ..., \left|\bar{\lambda}_n\right|\right)^T$, буде ближче до e_1, чим нормований вектор $\bar{\sigma}$ СНЧ A, тобто:

$$\angle\left(\bar{\lambda}, e_1\right) < \angle\left(\bar{\sigma}, e_1\right). \tag{17}$$

Співвідношення (17) приведе до того, що для матриці F ЦЗ буде більше блоків у вигляді B, для яких

$$\angle\left(\bar{u}_1, \bar{\lambda}\right) \approx \angle\left(n^\circ, e_1\right), \tag{18}$$

де $\bar{u}_1$ для матриці B є ВВ, який відповідає максимальному власному значенню $\bar{\lambda}_1$, ніж блоків оригінальних A, для яких має місце (1).

Таким чином нами доведено

Твердження 1. Для більшості блоків у симетричному вигляді (7), що ставляться у відповідність блокам оригінального ЦЗ, має місце співідношення (18), при цьому (18) виконується для більшої кількості блоків, ніж співвідношення (1) для оригінальних блоків зображення.

Поняття «більшості блоків ЦЗ» на практиці візуалізується модою гістограми, що далі позначається Γ_λ, значень кутів $\angle\left(\bar{u}_1, \bar{\lambda}\right)$ $l\times l$-блоків цього зображення, яка для оригінального ЦЗ, дорівнює значенню кута $\angle\left(n^\circ, e_1\right)$ у відповідному просторі R^l. З доказу твердження 1 випливає, що при порушенні цілісності ЦЗ мода Γ_λ може зсуватися з положення $\angle\left(n^\circ, e_1\right)$, що буде, разом з іншими характеристиками, вказівкою на неавторізовану зміну зображення. Крім зсуву моди Γ_λ на порушення цілісності ЦЗ буде вказувати зміна характеру гістограми: в результаті збурної дії, навіть якщо мода Γ_λ і залишиться в $\angle\left(n^\circ, e_1\right)$, значення в моді значно зменшиться, значна кількість блоків, що в оригінальному ЦЗ робили свій внесок в стовпець Γ_λ, що відповідає моді, в збуреному ЦЗ зробить внесок в інші стовпці. Оскільки відповідно до загальної формули для довільної симетричної матриці M :

$$\max_j \left|\lambda_j(M) - \lambda_j(M + \Delta M)\right| \le \|\Delta M\|_2, \tag{19}$$

де $M + \Delta M$ – збурена матриця, ΔM – матриця збурення, $\|\cdot\|_2$ – спектральна матрична норма [25], всі ВЗ симетричної $n\times n$-матриці M є добре обумовленими, таким же буде і вектор $\bar{\lambda}$ (16) симетричного блоку B (7), що ставиться у відповідність блоку A ЦЗ. Чутливість (обумовленість) ВВ $\bar{u}_1$ симетричної довільної M визначається формулою:

$$sin\ \theta_1 \le \frac{2\left\|\Delta M\right\|_2}{gap_{abs}(1, M)}, \qquad (20)$$

де θ_1 – гострий кут між ВВ, що відповідають максимальним ВЗ в матрицях M і $M + \Delta M$ Оскільки абсолютна відокремленість (15) максимального ВЗ для ЦЗ завжди є значною, такою, що набагато перевищує абсолютні відокремленості інших ВЗ, з (20) випливає нечутливість (добра обумовленість) $\bar{u}_1$ для блоку B (7). Віходячи з (19), (20), можна стверджувати, що для тих блоків, що в оригінальному ЦЗ робили свій внесок в стовпець Γ_λ, який відповідає моді $\angle(n^\circ, e_1)$, і для яких в результаті збурної дії значення кута $\angle(\bar{u}_1, \bar{\lambda})$ змінилося, ця зміна не може бути значною, залишаючи внесок таких блоків для збуреного ЦЗ в стовпці Γ_λ, що знаходяться в деякому незначному околі моди. Визначені зміни Γ_λ при змінах зображення будуть тим більше, чим більше буде величина збурної дії, якій піддалося ЦЗ.

Отримані теоретичні висновки знайшли своє підтвердження на практиці, ілюстрація чого для конкретного ЦЗ наведена на рис.1, де очевидним є збільшення значення гістограми Γ_λ в моді для випадку симетризованих блоків ЦЗ, яка відповідає значенню кута $\angle(n^\circ, e_1)$, що для 4×4 -блоків дорівнює 60 градусів (рис.1(б)), в порівнянні зі значенням в моді гістограми кутів між нормованим вектором СНЧ і лівим СНВ, що відповідає максимальному СНЧ, оригінальних блоків оригінального ЦЗ (рис.1(а)), а також видозміна Γ_λ при порушенні цілісності ЦЗ (рис.1(в,г)).

Враховуючи все наведене вище, пропонується наступний удосконалений відносно [11] універсальний метод виявлення порушення цілісності ЦЗ, основні кроки якого наступні:

Крок 1. Матриця F аналізованого ЦЗ розбивається стандартним чином на $l \times l$ -блоки, довільний з яких – блок A.

Крок 2. Кожному блоку A, отриманому на попередньому кроці, ставиться у відповідність симетричний блок $B = \frac{A + A^T}{2}$.

Крок 3. Для аналізованого ЦЗ будується гістограма Γ_λ значень кутів $\angle(\bar{u}_1, \bar{\lambda})$ в блоках B з кроком h.

Крок 4. Для гістограми Γ_λ визначається мода A_λ, а також значення M_λ в моді.

Крок 5. Для аналізованого ЦЗ з використанням Γ_λ обчислюється кількість S_λ блоків, для яких:

$$\angle(\bar{u}_1, \bar{\lambda}) \in \left[\angle(n^\circ, e_1) - T, \angle(n^\circ, e_1) + T\right],$$

де T – параметр, що визначається експериментально, характеризує радіус околa $\angle(n^\circ, e_1)$.

Крок 6 (*перевірка*).

Якщо

$$A_\lambda \notin \left\{\angle(n^\circ, e_1) - 1^\circ,\ \angle(n^\circ, e_1),\ \angle(n^\circ, e_1) + 1^\circ\right\},$$

то

для аналізованого ЦЗ цілісність порушена.

Якщо

$$\left(A_\lambda \in \left\{\angle\left(n^\circ, e_1\right) - 1^\circ,\ \angle\left(n^\circ, e_1\right),\ \angle\left(n^\circ, e_1\right) + 1^\circ\right\}\right) \& \left(S_\lambda / M_\lambda > P\right),$$

де P – порогове значення, що визначається експериментально, характеризує видозміну гістограми в результаті збурної дії,

то

для аналізованого ЦЗ цілісність порушена.

Якщо

$$\left(A_\lambda \in \left\{\angle\left(n^\circ, e_1\right) - 1^\circ,\ \angle\left(n^\circ, e_1\right),\ \angle\left(n^\circ, e_1\right) + 1^\circ\right\}\right) \& \left(S_\lambda / M_\lambda \le P\right),$$

то

для аналізованого ЦЗ цілісність не порушена.

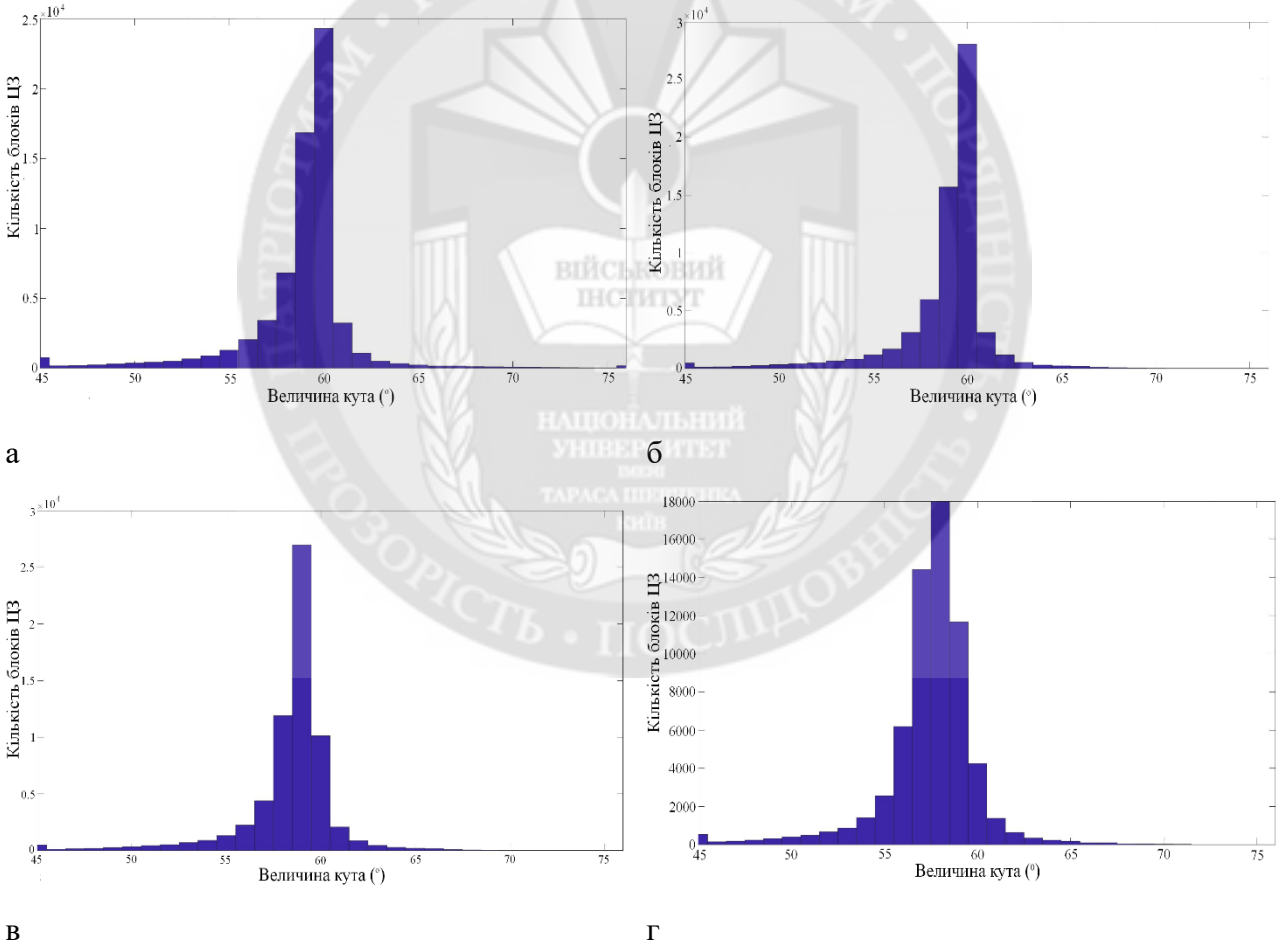


Рисунок 1 – Ілюстрація відмінностей відповідних гістограмм для конкретного ЦЗ

При його стандартному розбитті на 4×4-блоки: а – гістограма значень кутів між нормованим вектором СНЧ і лівим СНВ, що відповідає максимальному СНЧ, оригінальних

блоків оригінального ЦЗ; б – гістограма Γ_λ для оригінального ЦЗ; в, г – Γ_λ для ЦЗ, що піддалося збурній дії (мультиплікативний шум з $D = 0.001, 0.005$ відповідно).

Наслідком твердження 1 при реалізації удосконаленого методу буде збільшення показника TN (2) та незбільшення показника TP у порівнянні з первісним методом [11], що в результаті, виходячи з теоретичних міркувань, повинно привести до відносної порівнянності значень ACC для цих двох методів.

Подальші результати обчислювального експерименту приводяться для алгоритмічної реалізації методу при наступних значення параметрів: $T = 15^\circ$, $P = 3.2$, $h = 1^\circ$, $l \in \{4,8,16,32\}$. В обчислювальному експерименті, метою якого була оцінка, в тому числі порівняльна, ефективності алгоритмічної реалізації удосконалено методу, було задіяно 500 оригінальних ЦЗ розміром 1024×1024 пікселя.

Результати есперименту, який проводився з використанням двох комп'ютерів (К1, К2) різної конфігурації (табл.1), що стосуються оцінки часових витрат, наведено на рис.2 для $l \in \{4,8,16,32\}$. Отримані результати ілюструють значну часову перевагу запропонованого удосконалення методу для кожного розміру блоку, яка монотонно зростає зі зменшенням їх кількості. Для $l = 32$ зменшення часу на експертизу одного ЦЗ складає 36.4% (для К1) і 30% (для К2) в порівнянні з аналогічним параметром первісного методу (рис.2(б)), середнє ж значення для зменшення часу по всьому експерименту ($l \in \{4,8,16,32\}$) становить 28.6% (пристрій К1), 23.7% (пристрій К2).

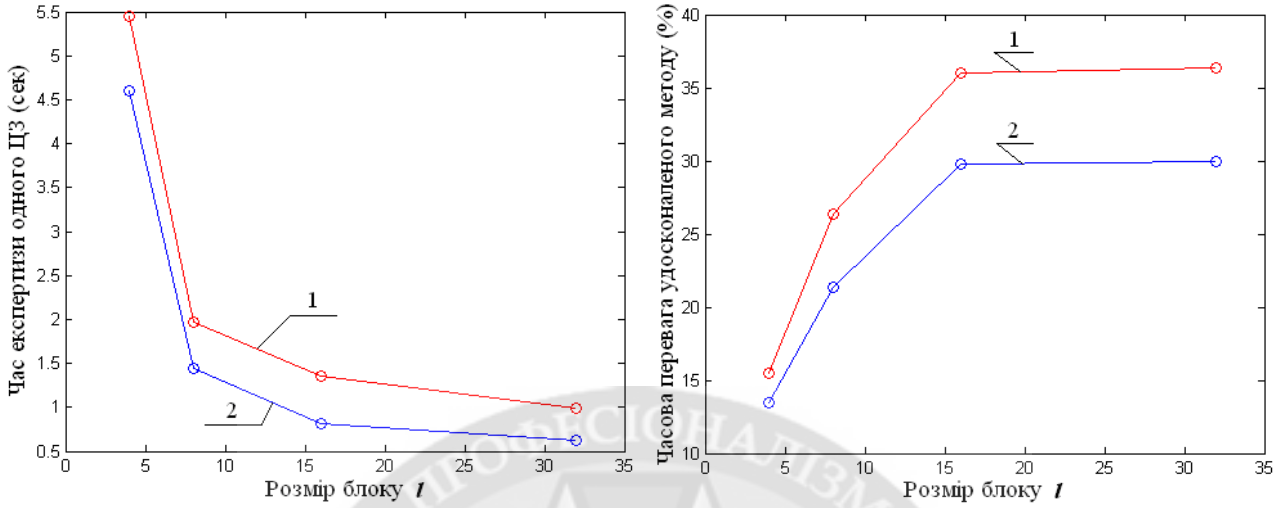
Зауваження. Треба зазначити, що наявні значні часові переваги удосконаленого методу відносно методу [11] досягаються не тільки в результаті меньшої обчислювальної складності безпосередньо спектрального розкладання симетризованих матриць блоків в порівнянні з сингулярним розкладанням оригінальних блоків, які відбуваються в ході експертизи, а й завдяки тому, що у вдосконаленому методі вдвічі зменшується кількість досліджуваних при експертизі об'єктів. Дійсно, в [11] будуються і досліджуються гістограми Γ_U, Γ_V кутів $\angle(u_1, \bar{\sigma})$, $\angle(v_1, \bar{\sigma})$ для першого лівого і першого правого СНВ відповідно, тоді як в запропонованому методі лише Γ_λ, оскільки спектральне розкладання симетричної матриці зменшує кількість параметрів, що визначають відповідну матрицю, в порівнянні з сингулярним.

Таблиця 1.

Характеристики обчислювальних пристроїв К1, К2, використаних при тестуванні алгоритмічної реалізації удосконаленого методу виявлення порушення цілісності ЦЗ

Пристрій	К1	К2
Ім'я пристроя	Aspire ES1-532G	LenovoIdeaPadGaming 3 15ACH6
RAM	4 ГБ	16 ГБ
Відеокарта	NVIDIA GeForce 920mx	NVIDIA GeForce RTX 3050 Ti
Об'єм відеокарти	2 ГБ	4 ГБ
Процесор	IntelPentium N3710	AMD Ryzen 5 5600H
Кількість ядер процесора	4	6
Кількість потоків процесора	4	12

Базова швидкість	1.6 Гц	3.3 Гц
Накопичувач	SSD 512 ГБ	SSD 512 ГБ



а б

Рисунок 2 – Порівняльна оцінка часових витрат експертизи ЦЗ: а – графіки залежності часу експертизи одного ЦЗ розміром 1024×1024 пікселя від розміру блоку l (показники К1): 1 – метод [11], 2 – удосконалений метод; б – графік залежності часової переваги удосконаленого методу над методом [11] від розміру блоку на експертизу одного ЦЗ (%) на пристрої: 1 – К1; 2 – К2.

Результат будь-якої збурної дії ΔF, спрямованої на ЦЗ з матрицею F, можна представити у вигляді [26]:

$$\overline{F} = F + \Delta F, \tag{21}$$

де $\overline{F}$ – матриця ЦЗ, цілісність якого порушена. З (21) випливає наявність нескінченної кількості різноманітних збурних дій, кожна з яких визначається своєю матрицею ΔF. З урахуванням практичної неможливості розгляду всієї різноманітності збурень, а також того, що результат будь-якої збурної дії загалом може розглядатися як накладання деякого шуму [28], при моделюванні збурних дій в роботі були використані різноманітні шуми з різними параметрами. Результати оцінки, зокрема порівняльної, точності виявлення порушення цілісності ACC (2) в таких умовах наведені в табл.2, де кращий результат в умовах конкретного значення l і конкретної збурної дії для наочності виділений жирним шрифтом.

Для наочності порівняння ефективностей методів визначимо:

$$R = \frac{ACC_2 - ACC_1}{ACC_1} \cdot 100\ \%, \tag{22}$$

де ACC_1, ACC_2 – значення параметру ACC для [11] і удосконаленого методу відповідно. Оцінка (22) знайшла своє відображення на рис.3, де очевидною є перевага удосконаленого методу для більшості збурних дій при різних розмірах блоків. Така перевага здебільшого пояснюється збільшенням параметру TN, що фігурує в (2). Це збільшення TN склало: 13.6, 19.6, 29.8, 26.8% для $l = 4, 8, 16, 32$ відповідно. Максимально підвищення точності виявлення ACC в

порівнянні з первісним методом склало 10.2%. І хоча для деяких збурних дій (гауссівський шум ($D = 0.0001, 0.001$)) при деяких значеннях l спостерігалось зменшення ACC (максимально це зменшення склало 6.2%), в цілому очевидним є підвищення точності виявлення порушення цілісності ЦЗ удосконаленим методом: середнє по експерименту значення R є додатним і складає 5.42%.

Таблиця 2.

Значення ACC в умовах різних збурних дій та різних розмірів, які використовуються при експертизі ЦЗ блоків

Збурна дія	Розмір блоку l	ACC	
		Метод [11]	Удосконалений метод
Мультиплікативний шум ($D = 0.005$)	4	0.8611	**0.9111**
	8	0.8056	**0.8722**
	16	0.7611	**0.8389**
	32	0.7278	**0.7889**
Гауссівський шум з нульовим математичним очікуванням ($D = 0.0001$)	4	0.5722	**0.5833**
	8	**0.5389**	0.5167
	16	0.5222	**0.5444**
	32	**0.5389**	0.5278
Гауссівський шум з нульовим математичним очікуванням ($D = 0.001$)	4	**0.8556**	0.8056
	8	0.8056	**0.8556**
	16	0.7556	**0.8056**
	32	0.7222	**0.7667**
Гауссівський шум з нульовим математичним очікуванням ($D = 0.01$)	4	0.8667	**0.9167**
	8	0.8111	**0.8722**
	16	0.7611	**0.8389**
	32	0.7278	**0.7889**
Пуассонівський шум	4	0.8667	**0.9111**
	8	0.8111	**0.8722**
	16	0.7611	**0.8389**
	32	0.7278	**0.7889**

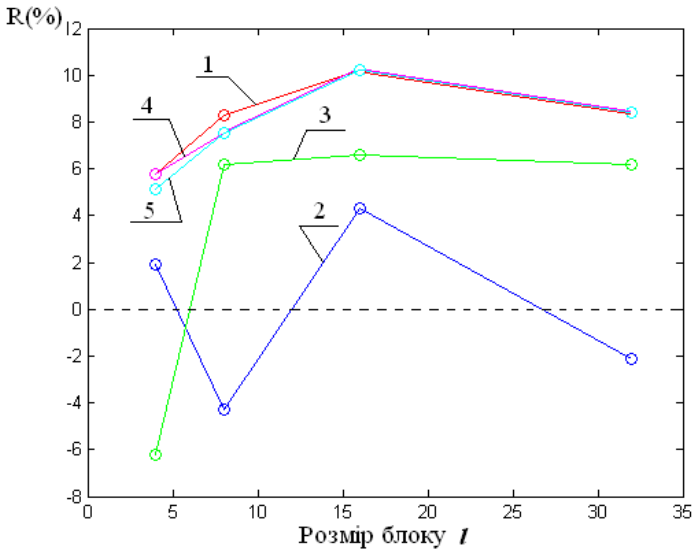


Рисунок 3 – Графіки залежності значення R (22) від розміру блоку в умовах різних збурних дій: 1 – мультиплікативний шум ($D = 0.005$); 2,3,4 – гауссівський шум з нульовим математичним очікуванням і $D = 0.0001$, $D = 0.001$ і $D = 0.01$ відповідно; 5 – пуассонівський шум

Таким чином, по результатам тестування алгоритмічної реалізації удосконаленого універсального методу виявлення порушення цілісності ЦЗ можна стверджувати, що його ефективність перевищує ефективність методу [11] як по обчислювальній складності (часу експертизи одного ЦЗ), так і по точності виявлення.

Висновки. В роботі вирішено важливу та актуальну науково-практичну задачу підвищення ефективності виявлення порушень цілісності ЦЗ шляхом удосконалення універсального методу, запропонованого в [11].

Мета роботи була досягнута завдяки теоретично обгрунтованому вибору способу симетризації матриці $l \times l$-блоку ЦЗ з наступним доведенням того, що для більшості отриманих симетричних блоків, що ставляться у відповідність блокам оригінального ЦЗ, кут між лексикографічно додатним власним вектором, що відповідає максимальному власному значенню симетризованого блока, і нормованим вектором модулів власних значень дорівнює куту між *n*-оптимальним та першим вектором e_1 стандартного базису відповідного простору R^l. Найбільш важливим результатом роботи є удосконалений універсальний метод виявлення порушення цілісності ЦЗ, готовий до практичної реалізації. Властивості аналізуємих параметрів, зменшення їх кількості в симетричних блоках дають можливість підвищити показник правильно виявлених оригінальних ЦЗ і, як наслідок, точність виявлення в середньому більше, ніж на 5%; зменшити обчислювальну складність і, як наслідок, часові витрати на експертизу ЦЗ в середньому більше, ніж на 23%, в порівнянні з [11].

В даний момент зусилля авторів роботи сконцентровані на уточненні параметрів, що використовуються при алоритмічній реалізації методу, для підвищення показника *TP* з наступним підвищенням точності виявлення порушення цілісності ЦЗ.

ЛІТЕРАТУРА:

1. Информационное противоборство в современных условиях / Л.Г. Пирцхалава, В.А. Хорошко, Ю.Е. Хохлачева, М.Е. Шелест. К.: ЦП «Компринт», 2019. 226 с.

2. Uliyan, D.M., Jalab, H.A., Abdul Wahab, A.W., Sadeghi, S. Image region duplication forgery detection based on angular radial partitioning and Harris key-points / Symmetry. 2016. 8(7). 62.

3. Задірака, В.К. Сучасні методи розв'язання задач інформаційної безпеки / Вісник НАН України. 2014. 5. С. 65–69.

4. Mandal, P.C., Mukherjee, I., Paul, G., Chatterji, B.N. Digital image steganography: A literature survey / Information Sciences. 2022. 609. P. 1451–1488.

5. Борисенко, І.І. Виявлення цифрового фотомонтажу на основі аналізу контрастності зображення / Сучасний захист інформації. 2020. №2. С. 47–51.

6. Joglekar, N.P., Chatur, P.N. A compressive survey on active and passive methods for image forgery detection / International Journal of Engineering and Computer Science. 2015. 4(1). P. 10187–10190.

7. Shwetha, B., Sathyanarayana, S.V. Digital image forgery detection techniques: a survey / ACCENTS Transactions on Information Security. 2017. 2(5). P. 22–31.

8. Thakur, T., Singh, K., Yadav, A. Blind approach for digital image forgery detection / International Journal of Computer Applications. 2018. 179(10). P. 34–42.

9. Chu, X., Li, H. A Survey of Blind Forensics Techniques for JPEG Image Tampering / Journal of Computer and Communications. 2019. 7(10). P. 1–13.

10. 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.

11. 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.

12. Lerch-Hostalot, D., Megias, D. Unsupervised steganalysis based on artificial training sets / Engineering Applications of Artificial Intelligence. 2016. 50. P. 45–59.

13. Bobok, I.I. Steganalysis method for detection of the hidden communication channel with low capacity / Telecommunications and Radio Engineering. 2018. 77(18). P. 1597–1604.

14. Лебедева, Е.Ю., Кобозева, А.А. Основы метода выявления клонированных участков изображения, подвергнутых коррекции яркости / Сучасна спеціальна техніка. 2013. 3(34). С. 17–24.

15. Li, H., Luo, W., Qiu, X., Huang, J. Image forgery localization via integrating tampering possibility maps / IEEE Transactions on Information Forensics and Security. 2017. 12(5). P. 1240–1252.

16. Трифонова, К.О. Метод виявлення порушення цілісності цифрового зображення шумом Перліна / Радіоелектроніка, інформатика, управління. 2017. 2. С. 134–142.

17. Khan, S., Khan, K., Ali, F., Kwak, K.-S. Forgery detection and localization of modifications at the pixel level / Symmetry. 2020. 12(1). 137.

18. Al-Jarrah, M.M, Al-Taie, Z.H., Abuarqoub, A. Steganalysis using LSB-focused statistical features / Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS'17). 2017. Article 54. P. 1–5.

19. Зоріло, В.В., Кіосєва, О.І., Зоріло, І.В. Модифікація алгоритму виявлення штучного підвищення різкості цифрового зображення / Інформатика та математичні методи в моделюванні. 2018. 8(2). С. 156–163.

20. Duan, X.T., Peng, T., Li, F.F., Wang, J. Blind separation of tampered images based on JPEG double compression properties / Journal of University of Jinan (Science and Technology). 2017. 31. P. 87–96.

21. Bobok, I.I., Kobozeva, A.A. Method for detecting of digital image integrity violations due to its block processing / Радіотехніка. 2019. 199. С. 130–141.

22. Geetha, S., Sindhu, S., Kamaraj, N. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / Transactions on Data Privacy. 2009. 1. P. 140–161.

23. Гонсалес, Р., Вудс, Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.

24. Bergman, C., Davidson, J. Unitary embedding for data hiding with the SVD / Security, steganography and watermarking of multimedia contents VII, SPIE. 2005. 5681. P. 619–630.

25. Деммель, Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.

26. Кобозева, А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений / Праці Одеського політехнічного університету. 2014. 2. С. 136–146.

27. Гантмахер, Ф.Р. Теория матриц: монография. 5-е изд. М.: Физматлит, 2004. 559 с.

28. Srinivas, R., Panda, S. Performance analysis of various filters for image noise removal in different noise environment / International Journal of Advanced Computer Research. 2013. 3. P. 47–52.

REFERENCES:

1. Pirtskhalava, L.G., Khoroshko, V.A., Khokhlacheva, J.E., Shelest, M.E. (2019), "Informatsionnoe protivoborstvo v sovremennyh usloviyah" [Information Warfare in Modern Conditions], Komprint, Kyiv, 226 p.

2. Uliyan, D.M., Jalab, H.A., Abdul Wahab, A.W., Sadeghi, S. (2016), "Image region duplication forgery detection based on angular radial partitioning and Harris key-points", Symmetry, 8(7), 62.

3. Zadiraka, V.K. (2014), "Suchasni metody rozvyazannya zadach informatsiynoy bezbeky" [Modern Methods for Solving the Tasks of Information Safety], Visnyk of the National Academy of Sciences of Ukraine, 5, pp. 65–69.

4. Mandal, P.C., Mukherjee, I., Paul, G., Chatterji, B.N. (2022), "Digital image steganography: A literature survey", Information Sciences, 609. pp. 1451–1488.

5. Borysenko, I.I. (2020), "Vyyavlennya tsyfrovogo fotomontazhu na osnovi kntrstnosti zobrazhennya" [Detection of digital photomontage based on image contrast analysis], Modern Information Security, 2, pp. 47–51.

6. Joglekar, N.P., Chatur, P.N. (2015), "A compressive survey on active and passive methods for image forgery detection", International Journal of Engineering and Computer Science, 4(1), pp. 10187–10190.

7. Shwetha, B., Sathyanarayana, S.V. (2017), "Digital image forgery detection techniques: a survey", ACCENTS Transactions on Information Security, 2(5), pp. 22–31.

8. Thakur, T., Singh, K., Yadav, A. (2018), "Blind approach for digital image forgery detection", International Journal of Computer Applications, 179(10), pp. 34–42.

9. Chu, X., Li, H. (2019), "A Survey of Blind Forensics Techniques for JPEG Image Tampering", Journal of Computer and Communications, 7(10), pp. 1–13.

10. Bobok, I.I. (2017), "Rozvytok zagalnogo pidhodu do problem vyyavlennya porushen' tsilisnosti tsyfrovyh zobrazhen" [Development of a general approach to the problem of detecting integrity violations of digital images] / Legal, Regulatory and Metrological Support of Information Security System in Ukraine, 2, pp. 78–88.

11. Kobozeva, A.A., Bobok, I.I., Garbuz, A.I. (2016), "General principles of integrity checking of digital images and application for steganalysis", Transport and Telecommunication Journal, 17(2), pp. 128–137.

12. Lerch-Hostalot, D., Megias, D. (2016), "Unsupervised steganalysis based on artificial training sets", Engineering Applications of Artificial Intelligence, 50, pp. 45–59.

13. Bobok, I.I. (2018), "Steganalysis method for detection of the hidden communication channel with low capacity", Telecommunications and Radio Engineering, 77(18), pp. 1597–1604.

14. Lebedieva, E.J., Kobozieva, A.A. (2013), "Osnovy metoda vyyavleniya klonirovannyh uchastkov izobrazheniy, podvergnutyh korrektsii yarkosti" [Fundamentals of the method for detecting cloned image areas subjected to brightness correction], Modern Special Technics, 3, pp. 17–24.

15. Li, H., Luo, W., Qiu, X., Huang, J. (2017), “Image forgery localization via integrating tampering possibility maps”, IEEE Transactions on Information Forensics and Security, 12(5), pp. 1240–1252.

16. Tryfonova, K.O. (2017), “Metod vyyavlennya porushennya tsilisnosti tsyfrovogo zobrazhennya shumom Perlina” [A method of detecting a violation of the integrity of a digital image by Perlin noise], Radio Electronics, Computer Science, Control, 2, pp. 134–142.

17. Khan, S., Khan, K., Ali, F., Kwak, K.-S. (2020), “Forgery detection and localization of modifications at the pixel level”, Symmetry, 12(1), 137.

18. Al-Jarrah, M.M, Al-Taie, Z.H., Abuarqoub, A. (2017), “Steganalysis using LSB-focused statistical features”, Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS’17), article 54, pp. 1–5.

19. Zorilo, V.V., Kioseva, O.I., Zorilo, I.V. (2018), “Modyfikatsiya algorytmu vyyavlennya shtuchnogo pidvyschennya rizkosti tsyfrovogo zobrazhennya” [Modification of algorithm for detecting artificial improvement of sharpness of the digital image], Informatics and Mathematical Methods in Simulation, 2, pp. 156–163.

20. Duan, X.T., Peng, T., Li, F.F., Wang, J. (2017), “Blind separation of tampered images based on JPEG double compression properties”, Journal of University of Jinan (Science and Technology), 31, pp. 87–96.

21. Bobok, I.I., Kobozeva, A.A. (2019), “Method for detecting of digital image integrity violations due to its block processing”, Radiotechnika, 199, pp. 130–141.

22. Geetha, S., Sindhu, S., Kamaraj, N. (2009), “Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images”, Transactions on Data Privacy, 1, pp. 140–161.

23. Gonzalez, R.C., Woods, R.E. (2006), “Tsifrovaya obrabotka izobrazheniy” [Digital Image Processing], Technosfera, Moscow, 1070 p.

24. Bergman, C., Davidson, J. (2005), “Unitary embedding for data hiding with the SVD”, Security, steganography and watermarking of multimedia contents VII, SPIE, 5681, pp. 619–630.

25. Demmel, D. (2001), “Vychislitelnaya linejnaya algebra: teoriya i prilozheniya” [Numerical Linear Algebra: Theory and Applications], Mir, Moscow, 430 p.

26. Kobozeva, A.A. (2014), “Osnovy obschego podhoda k razrabotke universalnyh steganoanaliticheskih metodov dlya tsifrovyh izobrazheniy” [A basis of common approach to the development of universal steganalysis methods for digital images], Odes’kyi Politechnichnyi Universytet. Pratsi, 2, pp 136–146.

27. Gantmacher, F.R. (2004), “Teoriya matrits: monografiya” [Matrix Theory], FizMatLit, Moscow, 559 p.

28. Srinivas, R., Panda, S. (2013), “Performance analysis of various filters for image noise removal in different noise environment”, International Journal of Advanced Computer Research, 3, pp. 47–52.

Doctor of Technical Sciences, Kobozieva A.A.,
Doctor of Technical Sciences, Maevsky D.,A.
Kyryliuk V.O.

METHOD OF DETECTING VIOLATION OF DIGITAL IMAGE INTEGRITY BASED ON SPECTRAL DECOMPOSITION OF SYMMETRIZED BLOCK MATRIX

The work considers an important scientific and practical task of increasing the effectiveness of detecting violations of the integrity of information, in particular digital images, which is its common representation, which is becoming one of the main ones for specialists in the field of information and cyber security today. Undetected, unauthorized changes to information in a timely manner can lead to negative, catastrophic consequences for individuals, enterprises, banks, firms, and for humanity as a whole, when it comes to information that constitutes a state secret, contains data from the military industry, nuclear energy, chemical industry, etc., which determines the relevance of the problem under consideration. The main result

of the work is an improved universal method for detecting violations of the integrity of a digital image, ready for practical implementation, the theoretical basis of which is based on the analysis of eigenvalues and eigenvectors of symmetric blocks of the image matrix, which correspond to the original blocks. The paper substantiates the method of symmetrization of the block matrix, which allows to significantly (by more than 23%) reduce computational and, as a result, time costs for image examination in comparison with the time costs of the prototype method. It is proved that for the majority of the obtained symmetric blocks that correspond to the blocks of the original CG, the angle between the eigenvector corresponding to the maximum eigenvalue of the block and the normalized vector of the modules of the eigenvalues is equal to a certain value that does not depend on the specifics of the original image, but is sensitive to its changes, which made it possible to ensure the universality of the method and increase its efficiency in the sense of the accuracy of detecting a violation of the integrity of the image by more than 5%, compared to the analogue. The significance of the obtained results lies in ensuring, due to the use of the proposed method, an increase in the efficiency of the process of detecting violations of the integrity of the image according to the criteria of computing (time) costs for the examination of one image and the accuracy of detection.

Keywords: digital image, integrity violation, eigenvector, eigenvalue.