

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ БЛОКІВ МАТРИЦІ ЦИФРОВОГО КОНТЕНТУ В РІЗНИХ ФОРМАТАХ ЗБЕРЕЖЕННЯ ЯК ТЕОРЕТИЧНА ОСНОВА ДЛЯ МЕТОДІВ ВИЯВЛЕННЯ ПОРУШЕННЯ ЙОГО ЦІЛІСНОСТІ

Несанкціоновані зміни цифрових інформаційних контентів, зокрема зображень, відео, що розглядаються в роботі, сьогодні стають такими, виявлення яких є складною і актуальною задачею, що потребує розробки нових підходів та методів. При несанкціонованих змінах цифрового контенту часто відбувається зміна формату (з/без втрат) його збереження (в цілому, або частини), зокрема при організації стеганографічного каналу зв'язку, фотомонтажі тощо. Таким чином, виявлення факту перезбереження (частини) цифрового контенту в формат, що відрізняється від первісного, є показником на порушення його цілісності, роблячи актуальною задачу відокремлення контентів в різних форматах. Метою роботи є створення теоретичного базису для методів відокремлення цифрових контентів в різних форматах збереження шляхом дослідження властивостей формальних параметрів блоків оригінальних контентів. В ході дослідження: визначені формальні параметри – найменші за значенням сингулярні числа блоків відповідних матриць, на основі властивостей яких обґрунтована пропозиція введення формального об'єкта дослідження – матриці найменших сингулярних чисел блоків, що ставиться у відповідність цифровому контенту і має властивості, які розрізняються в залежності від формату збереження цифрового контенту; для послідовності цифрових зображень одного формату, для цифрового відео визначений формальний математичний об'єкт – гістограма мод гістограм матриць найменших сингулярних чисел блоків зображень/кадрів відео, властивості якої значно розрізняються для різних форматів збереження, що може бути використаним для розробки відповідного експертного методу. Встановлення кількісних характеристик для отриманих в роботі якісних роздільників дасть можливість сформулювати ефективні методи відокремлення цифрових контентів в різних форматах збереження, що може бути застосованим як складова частина процесу стеганоаналізу, в процесі виявлення результатів фотомонтажу, де були задіяні контенту в різних форматах, тощо.

Ключові слова: цифрове зображення, цифрове відео, формат з втратами, формат без втрат, сингулярне число

Вступ. Несанкціоновані зміни цифрових інформаційних контентів, зокрема цифрових зображень (ЦЗ), цифрових відео (ЦВ), що розглядаються в роботі, на сьогоднішній день стають дуже якісними, легко реалізуються існуючими програмними засобами, надзвичайно поширеними, такими, виявлення яких є складною і актуальною задачею, що потребує розробки нових підходів та методів, удосконалення існуючих [1–3].

Збереження ЦЗ/ЦВ може відбуватися з використанням двох принципово різних схем: з втратами та без втрат [4]. Збереження з втратами, з урахуванням особливостей людського зору, відбувається завдяки зменшенню (аж до обнуління) високочастотної складової відповідного сигналу [5], що відбивається на формальних параметрах цифрового контенту. При несанкціонованих змінах ЦЗ/ЦВ часто відбувається зміна його формату в цілому, або зміна формату частини ЦЗ/кадру ЦВ. Перший варіант часто виникає при організації прихованого (стеганографічного) каналу зв'язку [6]. Враховуючи лавиноподібне збільшення обсягу інформаційного контенту, який зберігається, передається каналами зв'язку, обробляється за допомогою комп'ютерної техніки, що відбувається останнім часом, цей контент, як правило, створюється в форматах з втратами. Це приводить до того, що як контейнер сьогодні найчастіше

використовується ЦЗ/ЦВ в форматі збереження з втратами. Якщо вбудова додаткової інформації робиться стеганометодом, який не є стійким до атаки стиском, наприклад, методом модифікації найменшого значущого біта, що є одним з найпоширеніших стеганографічних методів в сучасному інформаційному просторі [7], це потребує збереження отриманого стеганоповідомлення в форматі без втрат, що приводить до зміни первісного формату контейнера [8]. Другий варіант має місце, коли порушення цілісності цифрового контенту відбувається локально, зокрема при фотомонтажі, при цьому контенти, що використовуються, мають різні (з/без втрат) формати [9,10].

Таким чином, виявлення факту перезбереження ЦЗ/ЦВ в формат, що відрізняється від первісного, чи наявність в ЦЗ/кадрі ЦВ частин, властивості яких відрізняються в сенсі формату збереження, є показником на порушення цілісності цифрових контентів, роблячи актуальною задачу відокремлення їх в різних (з/без втрат) форматах.

Аналіз останніх досліджень і публікацій. Питання відокремлення цифрових контентів (ЦК) в різних форматах збереження не є новим серед наукової світової спільноти. Підходи до рішення задачі, що розглядається, у випадку ЦЗ та ЦВ принципово не розрізняються, оскільки ЦВ формально може бути представленим як послідовність ЦЗ – кадрів відео. В [11] розглядається питання виявлення блокової обробки ЦЗ, частковим випадком якої є його збереження з втратами. Автори використовують градієнтний аналіз, встановлюючи факт збільшення величини градієнта уздовж границь блоків, на які розбивається матриця ЦЗ. Але основна увага авторів приділяється визначенню розміру використовуваних при обробці зображення блоків, що негативно впливає на ефективність виявлення за допомогою запропонованого підходу результату стиску ЦК. В [12] автори також зосереджені на пошуку артефактів від блокової обробки зображення, запронований метод виявлення якої використовує кросс-диференційний фільтр для визначення границь усіх можливих блокових артефактів, морфологічні операції для видалення граничних ефектів, викликаних краями фактичного вмісту зображення, оцінку максимальної правдоподібності. Кожний з наведених вище методів [11,12], будучи практично ефективним, поступається в оцінці ефективності методу виявлення блокової обробки ЦЗ, запропонованому в [13], заснованому на аналізі властивостей гістограми значень кутів між нормованим вектором квадратів сингулярних чисел блоків матриці ЦЗ і лівим/правим сингулярним вектором, що відповідає максимальному сингулярному числу блока, при використанні цього методу для відокремлення ЦЗ в різних (з/без втрат) форматах збереження. При цьому значною перевагою методу є те, що точність виявлення порушення цілісності ЦЗ за рахунок його стиску із втратами залишається тут не тільки високою, а й практично не залежить від коефіцієнту якості QF , що використовувався під час стиску. Треба все ж зазначити, що методи, налаштовані на виявлення будь-якої блокової обробки цифрового контенту, що є в цьому сенсі універсальними, а не розрахованими саме на конкретну збурну дію – виявлення результату стиску з втратами, якими є вище розглянуті методи, принципово не можуть бути настільки ж ефективними при його виявленні, як спрямовані, тобто такі, що налаштовані саме на відокремлення ЦК в різних (з/без втрат) форматах. Безпосередньо питання відокремлення ЦЗ в різних форматах збереження розглядається в [9]. Це питання тут розв'язується з метою використання результатів відокремлення для виявлення фотомонтажу, що робиться за допомогою аналізу властивостей матриці нульових сингулярних чисел блоків, які відрізняються для ЦЗ в форматах з/без втрат. При формуванні згаданої матриці кожному блоку ЦЗ ставиться у відповідність число, що визначає кількість нульових сингулярних чисел цього блоку. Але треба зазначити, що для оригінальних ЦЗ в $l \times l$ -блоках, де $l \geq 8$, навіть у форматі з втратами (з практично використовуваними коефіцієнтами якості $70 \leq QF \leq 80$) наявність сингулярних чисел, які в точності дорівнюють 0, є скоріше винятковою, ніж системною ситуацією, завдяки наявності округлень, що відбуваються при переведенні (блоку) зображення з частотної області в просторову. Крім цього, обчислення значень сингулярних чисел в системі чисел з плаваючою

точкою відбувається в умовах накопичення обчислювальної похибки, що робить нетривіальною задачу визначення таких, які в точності дорівнюють нулю. Більше того, завдяки особливостям машинної арифметики, тут можлива ситуація, коли дійсно нульове значення буде отриманим як додатне. Таким чином, аналіз матриці нульових сингулярних чисел блоків для відокремлення ЦЗ в різних форматах часто приводить до ускладнень, а підхід потребує удосконалення. В [14] запропонований метод виявлення факту стиску з втратами в кольорових ЦЗ, що дозволяє відокремити зображення, спочатку збережені у форматах без втрат, від зображень, перезбережених у формат без втрат з форматів з втратами, який аналізує просторову область ЦЗ. Розроблений метод заснований на врахуванні послідовних колірних триад триплетів у матриці унікальних кольорів і може бути використаний для визначення формату вхідного контейнера при стеганоаналізі, але, оскільки для використовуваного підходу критичним є розмір досліджуваної частини ЦЗ, то його використання очевидно не буде ефективним при виявленні фотомонтажу, де використовуються зображення в різних (з/без втрат) форматах. Конкретний метод відокремлення ЦЗ в різних форматах збереження, заснований на аналізі кутів між нормованим вектором сингулярних чисел блоків досліджуваного ЦЗ і першим вектором стандартного базису відповідного простору, був запропонований в [15]. Метод в цілому по ефективності перевищив існуючі аналоги, забезпечуючи лише 0.5% помилок першого роду (ЦЗ, яке було перезбережене у формат без втрат з формату з втратами, визначалося як оригінальне в форматі без втрат), 5% помилок другого роду (оригінальне ЦЗ визначалося як таке, формат якого був змінений), але наявність помилок тут не дає можливості говорити про остаточний розв'язок задачі, що розглядається.

Таким чином, не зважаючи на кількість існуючих різноманітних методів і підходів до задачі відокремлення ЦК в різних форматах збереження, ця задача не є вирішеною остаточно, залишаючи актуальним пошук нових математичних базисів для організації процесу відокремлення. Підвищення ефективності розв'язку саме цієї задачі буде сприяти підвищенню ефективності виявлення порушення цілісності ЦК в цілому, зокрема в процесі стеганоаналізу, виявлення фотомонтажу тощо.

Мета роботи та задачі дослідження. Нещодавно українськими науковцями був запропонований загальний підхід до аналізу стану інформаційних систем (ЗПАІС), заснований на матричному аналізі та теорії збурень [16], який добре зарекомендував себе при розв'язку задач виявлення порушення цілісності цифрових контентів, сьогодні отримує подальший розвиток та удосконалюється [17]. Враховуючи це, *метою* роботи є створення теоретичного базису для методів відокремлення ЦЗ/ЦВ в різних (з/без втрат) форматах збереження шляхом дослідження властивостей формальних параметрів блоків оригінальних ЦК на основі ЗПАІС.

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

1. Визначити в межах ЗПАІС формальні параметри ЦК, властивості яких потенційно дають змогу для відокремлення контентів в різних (з/без втрат) форматах збереження;
2. Встановити властивості матриці найменших сингулярних чисел блоків (МНСЧ), що ставиться у відповідність ЦЗ/кадру ЦВ, які розрізняються в залежності від формату збереження ЦК;
3. Визначити та дослідити математичний об'єкт, аналіз якого дасть можливість ефективно визначати формат ЦВ/послідовності ЦЗ, збережених в одному форматі.

Основний матеріал дослідження. Якісно формати збереження ЦК (з/без втрат) відрізняються ступенем присутності в блоках результуючого контенту високочастотної (середньочастотної) складової [4,5]. Саме квантування і округлення до цілих значень частотних коефіцієнтів блоків відповідних матриць, наслідком чого є обнуління високочастотних (можливо і середньочастотних) коефіцієнтів, приводить до стиску ЦК з втратами. У відповідності з ЗПАІС, стан (зміну стану) будь-якої інформаційної системи, частковим випадком якої є ЦЗ/(кадр) ЦВ, можна оцінити за допомогою аналізу (збурень) повного набору формальних параметрів, що визначають цю систему однозначно: сингулярних

чисел (СНЧ) і сингулярних векторів (СНВ) спеціального виду [18] відповідної матриці (матриць), що використовується далі в роботі.

Нехай F – матриця ЦЗ/кадру ЦВ. Враховуючи мету дослідження, блокову обробку контенту при збереженні в форматі з втратами, матриця F стандартним чином [5] розбивається на непересічні $l \times l$ -блоки, довільний з яких позначатиметься B . Побудова для кожного блоку B нормального сингулярного розкладання [18]:

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

де U, V – ортогональні $l \times l$ -матриці, стовпці яких $u_i, v_i, i = \overline{1, l}$, є лівими і правими СНВ B відповідно, при цьому ліві СНВ є лексикографічно додатними; $\Sigma = \text{diag}(\sigma_1, \dots, \sigma_l), \sigma_1 \geq \dots \geq \sigma_l \geq 0$ – СНЧ B , визначає однозначно повний набір його формальних параметрів. При цьому для блоків оригінального ЦЗ має місце співвідношення:

$$\sigma_1 \gg \sigma_2 \geq \dots \geq \sigma_l \geq 0. \quad (2)$$

Відповідно з ЗПАІС стан і властивості ЦЗ/кадру ЦВ тут буде визначатися сукупністю СНЧ і СНВ всіх блоків його матриці. Різниця в ступені наявності високочастотної (середньочастотної) складової в ЦЗ/кадрі ЦВ в різних форматах відіб'ється на складових повного набору формальних параметрів. Враховуючи, що високочастотній складовій ЦК відповідають головним чином сингулярні трійки (σ_i, u_i, v_i) з найменшими СНЧ [9,16], а саме їх значні зміни в результаті квантування і округлення частотних коефіцієнтів блоків, що відображаються в зменшенні найменших СНЧ блоків аж до обнуління [9], саме аналіз таких трійок потенційно може привести до розв'язку задачі, що розглядається.

Збурення сингулярних трійок (σ_i, u_i, v_i) в результаті стиску приведе до змін як СНЧ σ_i , так і СНВ u_i, v_i , але навіть після збурень СНВ залишаться попарно ортогональними, нормованими, ліві – лексикографічно додатними, лише змінивши свій напрям. При цьому, враховуючи (2), СНВ, які відповідають найменшим СНЧ, є чутливими до збурних дій у відповідності зі співвідношенням [19]:

$$\frac{1}{2} \sin 2\theta_i \leq \frac{\|\Delta B\|_2}{\text{svdgap}(i, B)}, \quad (3)$$

де ΔB – матриця збурення блоку B в результаті збурної дії, що зазнало ЦЗ, θ_i – кут повороту вектора u_i , $\text{svdgap}(i, B) = \min_{j \neq i} |\sigma_i - \sigma_j|$ – відокремленість СНЧ σ_i в блоці B , $\|\bullet\|_2$ – спектральна матрична норма.

Для значної кількості блоків ЦЗ/кадрів ЦВ найменші СНЧ за значенням не перевищують одиницю, маючи і відокремленість менше 1, роблячи відповідні СНВ у відповідності з (3) чутливими навіть до похибок округлення. Це приводить до того, що величина куту їх повороту (яка буде значною навіть при незначних збурних діях) не є інформативною з точки зору задачі, що розглядається. В той час, як збурення найменших СНЧ, що є нечутливими до збурних дій відповідно до співвідношення [19]:

$$\max_i |\sigma_i(B) - \sigma_i(B + \Delta B)| \leq \|\Delta B\|_2, \quad (4)$$

в результаті стиску з втратами має чітко виражений специфічний характер [9] – зменшення цих СНЧ аж до обнуління. Оскільки сингулярні трійки з найменшими СНЧ відповідають, головним чином, високочастотній складовій сигналу, то обнуління цієї складової в результаті стиску, враховуючи невід’ємність (2) СНЧ, може привести лише до їх зменшення. Дійсно, сингулярне розкладання блоку (1) може бути представленим у формі зовнішніх добутоків [19]:

$$B = \sum_{i=1}^l \sigma_i u_i v_i^T, \quad (5)$$

відповідно до якого сигнал B розкладається на суму однорангових сигналів, кожний з яких визначається своєю сингулярною трійкою (σ_i, u_i, v_i) . Одною з основних характеристик сигналу з матрицею B є його енергія E , яка може бути обчислена у відповідності з формулами [20]:

$$E = \sum_{i=1}^l \sum_{j=1}^l b_{ij}^2 = \sum_{u=0}^{l-1} \sum_{v=0}^{l-1} P(u, v), \quad (6)$$

де b_{ij} – елементи B , $P(u, v)$, $u = \overline{0, l-1}$, $v = \overline{0, l-1}$ – енергетичний спектр сигналу B . Позначимо результат дискретного косинусного перетворення (ДКП), яке є основним в найпоширенішому алгоритмі стиску з втратами для ЦЗ Ірег, блоку B як B_{DCT} . Елементи матриці B_{DCT} – коефіцієнти ДКП блоку B позначатимемо $B_{DCT}(u, v)$, $u = \overline{0, l-1}$, $v = \overline{0, l-1}$, тоді [5]: $P(u, v) = B_{DCT}^2(u, v)$.

У відповідності з (5) енергія сигналу B представляється у вигляді суми енергій $E(\sigma_i u_i v_i^T)$ сигналів $\sigma_i u_i v_i^T$:

$$\begin{aligned} E(\sigma_i u_i v_i^T) &= E \left(\sigma_i \begin{pmatrix} u_{1i} \\ u_{2i} \\ \vdots \\ u_{li} \end{pmatrix} (v_{1i} \ v_{2i} \ \dots \ v_{li}) \right) = E \left(\sigma_i \begin{pmatrix} u_{1i} v_{1i} & u_{1i} v_{2i} & \dots & u_{1i} v_{li} \\ u_{2i} v_{1i} & u_{2i} v_{2i} & \dots & u_{2i} v_{li} \\ \dots & \dots & \dots & \dots \\ u_{li} v_{1i} & u_{li} v_{2i} & \dots & u_{li} v_{li} \end{pmatrix} \right) = \\ &= \sigma_i^2 (u_{1i}^2 v_{1i}^2 + u_{1i}^2 v_{2i}^2 + \dots + u_{1i}^2 v_{li}^2 + u_{2i}^2 v_{1i}^2 + u_{2i}^2 v_{2i}^2 + \dots + u_{2i}^2 v_{li}^2 + \dots + u_{li}^2 v_{1i}^2 + u_{li}^2 v_{2i}^2 + \dots + u_{li}^2 v_{li}^2) = \\ &= \sigma_i^2 (u_{1i}^2 (v_{1i}^2 + v_{2i}^2 + \dots + v_{li}^2) + u_{2i}^2 (v_{1i}^2 + v_{2i}^2 + \dots + v_{li}^2) + \dots + u_{li}^2 (v_{1i}^2 + v_{2i}^2 + \dots + v_{li}^2)) = \\ &= \sigma_i^2 (u_{1i}^2 \|v_i\|^2 + u_{2i}^2 \|v_i\|^2 + \dots + u_{li}^2 \|v_i\|^2) = \sigma_i^2 \|u_i\|^2 \|v_i\|^2, \end{aligned}$$

де $\|\cdot\|$ – евклідова векторна норма.

Враховуючи властивості СНВ, що вимагаються в (1), (5), тобто: $\|u_i\| = \|v_i\| = 1$, $\forall i = \overline{1, l}$, маємо:

$$E(\sigma_i u_i v_i^T) = \sigma_i^2. \quad (7)$$

З (5), (6), (7) випливає:

$$\sum_{u=0}^{l-1} \sum_{v=0}^{l-1} B_{DCT}^2(u, v) = \sum_{i=1}^l \sigma_i^2.$$

Обнуління $B_{DCT}(u, v)$ для значень u, v , близьких до $l-1$, приведе до обнуління σ_i , коли i близько до l . Кількість найменших СНЧ, які підпадуть під такий результат, залежить від коефіцієнтів використовуваної при стиску матриці квантування, тобто від коефіцієнту якості QF стиску.

Таким чином, для розв'язку задачі, що розглядається, має сенс аналізувати сукупність найменших за значенням СНЧ блоків матриці ЦЗ/кадру ЦВ. Треба зазначити, що такий вибір досліджуваних параметрів дозволить уникнути необхідності застосування для їх обчислення саме нормального сингулярного розкладання, задовольнившись лише звичайним [19], яке дає можливість визначити однозначно СНЧ, але в обчислювальному сенсі є менш затратним, чим нормальне, оскільки не вимагає забезпечення лексикографічної додатності лівих СНВ.

Враховуючи досвід попередніх досліджень, заснованих на ЗПАІС [9], та недоліки застосування їх результатів, вказані вище, поставимо ЦЗ/кадру ЦВ з $n \times m$ -матрицею F у

відповідність матрицю найменших СНЧ блоків (МНСЧ) M_F розміром $\left[\frac{n}{l}\right] \times \left[\frac{m}{l}\right]$, де $[\cdot]$ – ціла

частина аргументу, з елементами $m_{(kp)_F}, k=1, \left[\frac{n}{l}\right], p=1, \left[\frac{m}{l}\right]$, які відповідають блокам F ,

наступним чином: $m_{(kp)_F}$ дорівнює кількості таких СНЧ σ_i відповідного блоку B , для яких виконується умова:

$$\sigma_i < T, \quad (8)$$

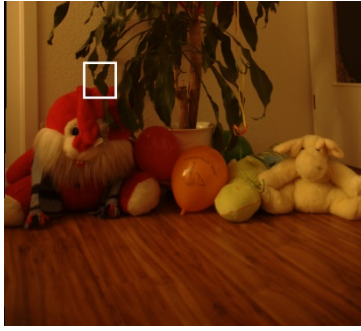
Слід зазначити, що для оригінальних ЦЗ/кадрів ЦВ при їх збереженні з втратами використовуються блоки розміром 8×8 пікселів, при цьому, як правило, в цих блоках найменше СНЧ $\sigma_8 < 1$, а для великої кількості блоків

$$\sigma_8 \ll 1 \quad (9)$$

в результаті обнуління високочастотної складової, тоді як в відповідних блоках цифрових контентів в форматі без втрат співвідношення (9) має місце в значно меншій кількості, оскільки там високочастотна складова має первісний вигляд [9]. Зрозуміло, що при зменшенні коефіцієнта якості стиску кількість СНЧ, які задовольняють (8), (9) буде збільшуватися, в той час, як з СНЧ контенту без втрат нічого відносно їх первісного значення відбуватися не буде. Враховуючи це, параметр в (8) для забезпечення можливості відокремлення ЦЗ/кадру ЦВ в різних форматах збереження в результаті аналізу МНСЧ має сенс обирати в межах:

$$0 < T < 1, \quad (10)$$

для того, щоб виявити кількість таких СНЧ, які в результаті квантування і округлення частотних коефіцієнтів $l \times l$ -блоків були нулями (порівнянними з нулем), а в досліджуваному ЦЗ/кадрі ЦВ відрізняються від нуля в результаті округлень, що відбуваються із значеннями яскравості пікселів при переході з частотної області в просторову. Враховуючи вище зазначене, можна стверджувати, що в цілому елементи МНСЧ для цифрових контентів в форматі з втратами будуть неменшими за елементи МНСЧ відповідного ЦЗ в форматі без втрат, при цьому відповідними будемо називати ЦЗ, як відрізняються лише форматом збереження (з/без втрат), відображаючи одну й ту саму сцену. Приклад МНСЧ при $T = 0.1$, що ілюструє істинність останнього твердження, наведено на рис.1 для відповідних ЦЗ.



а



б

1	0	1	1	1	0	1	1	1	1	1	0	1	1	0	0	1	0	0	1
1	0	1	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1
0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	2
1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0
0	1	1	0	0	0	0	1	0	0	0	1	0	1	0	1	0	0	1	1
0	0	0	1	0	1	1	1	0	0	1	0	1	0	1	1	1	1	1	1
1	0	0	0	1	1	0	0	1	0	1	0	0	0	0	1	1	1	0	0
1	0	0	0	1	0	0	0	0	1	1	0	1	1	1	0	1	1	0	1
1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0
1	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0
0	0	1	1	1	0	1	0	1	1	0	1	1	0	1	0	1	1	0	1
1	0	0	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	1
0	0	0	1	0	1	0	0	1	0	0	0	1	0	0	1	0	1	1	1
1	2	0	1	1	0	1	1	1	0	0	0	0	1	0	1	1	1	1	1
1	0	0	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	1	0
0	0	1	0	2	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
0	0	0	1	0	1	1	1	1	0	1	1	1	0	1	0	1	0	0	1
0	1	0	0	0	0	1	1	0	0	1	1	1	0	1	0	1	0	0	0
1	0	1	1	1	0	1	1	1	1	0	0	0	1	1	0	1	0	0	0

в

0	0	0	1	3	6	7	6	1	0	0	0	1	0	5	3	0	0	1	1
1	1	0	0	1	2	2	2	0	1	0	1	0	1	2	0	0	0	0	1
1	1	0	0	0	0	0	1	0	0	1	0	1	0	4	1	1	1	1	0
1	0	0	0	1	1	0	0	0	0	1	0	2	3	0	0	1	1	1	1
0	1	2	0	1	0	1	1	0	1	0	0	3	7	1	0	1	1	0	0
0	0	1	0	0	1	0	0	1	0	2	3	6	6	2	1	0	0	0	1
1	1	0	1	1	0	1	1	0	1	1	7	7	6	1	0	1	1	0	0
0	0	1	1	3	1	0	0	1	1	6	6	3	2	0	0	0	0	1	0
0	1	1	0	3	1	0	1	1	1	6	6	2	0	1	0	1	0	1	0
0	1	1	1	0	1	1	0	0	0	2	2	2	0	1	1	0	1	0	1
1	1	1	1	1	1	0	1	1	2	0	2	2	1	0	1	1	1	1	1
0	0	1	0	1	1	0	1	1	2	2	4	4	2	0	0	0	1	1	1
0	1	1	0	1	2	0	0	0	7	7	5	6	0	0	0	0	0	0	1
0	1	1	1	1	1	0	0	0	2	5	6	6	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0	0	0	2	6	6	2	0	0	1	1	0	0
1	0	1	1	0	2	1	0	0	0	0	5	6	0	1	1	0	1	0	0
0	0	1	1	0	2	1	1	1	0	1	2	7	0	1	0	0	0	0	1
1	1	1	1	0	0	1	0	0	1	1	0	1	2	0	0	0	1	0	1
2	1	2	1	1	0	1	1	0	1	1	0	0	1	1	0	0	0	0	1
1	2	1	1	2	1	0	1	0	2	1	0	1	3	0	0	1	1	1	0

г

Рисунок 1. Ілюстрація результату побудови МНСЧ для конкретного ЦЗ: а – тестове ЦЗ з виділеною частиною; б – частина ЦЗ, для якої формувалася МНСЧ ($T=0.1$); в – МНСЧ (ЦЗ в форматі Tif); г – МНСЧ (відповідне ЦЗ в форматі Jpeg ($QF = 75$))

Очевидно, маючи МНСЧ, що відповідають цифровим контентам в різних форматах збереження, визначитися з форматом кожного з них, порівнюючи між собою МНСЧ, не представляє труднощів, але питання визначення формату, як правило, вирішується для конкретного ЦК, коли в розпорядженні експерта є лише одна МНСЧ і треба мати можливість оцінити властивості цієї одної матриці, щоб зробити висновок про формат досліджуваного контенту. Зрозуміло, що значення елементів МНСЧ, яке найчастіше зустрічається для ЦЗ/кадру ЦВ в форматі з втратами, буде не менше за аналогічне значення для відповідного ЦЗ/кадру ЦВ в форматі без втрат; максимальне значення M_F , що відповідає контенту в форматі з втратами теж буде не менше за аналогічне значення для відповідного контенту в форматі без втрат, що ілюструє типовий приклад конкретних відповідних ЦЗ, одне з яких в

форматі Tif, а три інших (відповідних) отримані шляхом Perezберження першого в формат Jpeg з $QF \in \{70,75,80\}$ (найпоширеніші на практиці коефіцієнти якості) (рис.2).

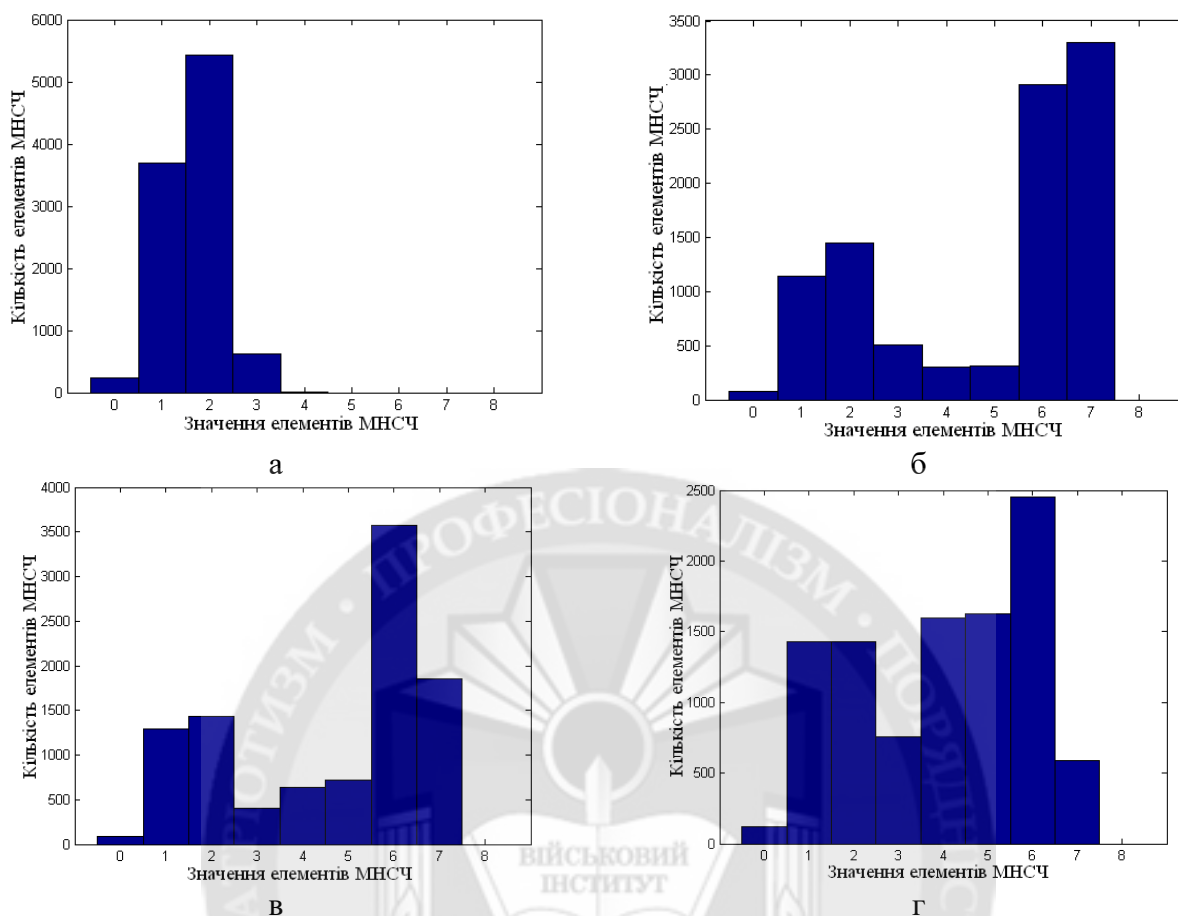
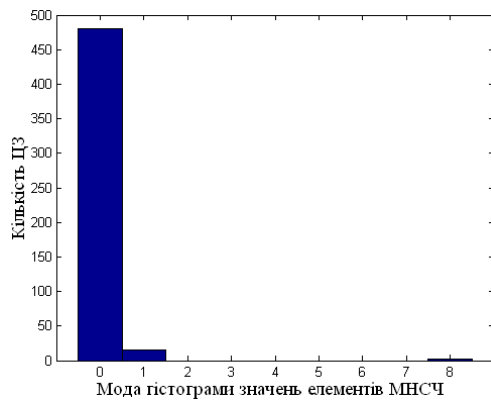
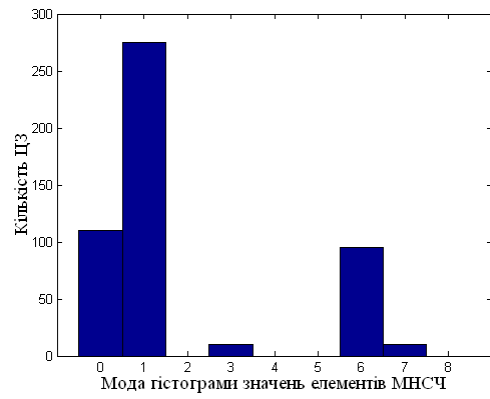


Рисунок 2. Гістограми елементів МНСЧ ($T = 0.5$) відповідних ЦЗ: а – в форматі без втрат (Tif); б, в, г – в форматі з втратами (Jpeg, $QF = 70,75,80$ відповідно)

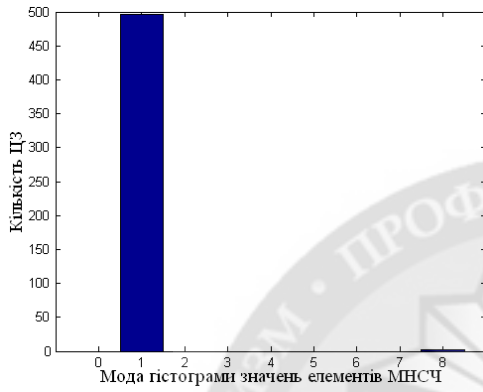
Подібна картина співвідношення гістограм значень елементів МНСЧ для ЦЗ/кадрів ЦВ в форматі з втратами та без втрат спостерігається для більшості відповідних ЦК: моди гістограм розрізняються по своєму значенню, збільшуючись для контенту в форматі з втратами, в порівнянні з ЦК без втрат, крім цього, мода гістограми не зменшується при зменшенні коефіцієнта якості стиску, практичним підтвердженням чого є результати обчислювального експерименту, частково наведені на рис.3 для Jpeg з $QF = 75$ (при інших значеннях коефіцієнта QF якісна картина для мод гістограм залишається такою ж, що повністю відповідає теоретичним очікуванням) та рис.4.



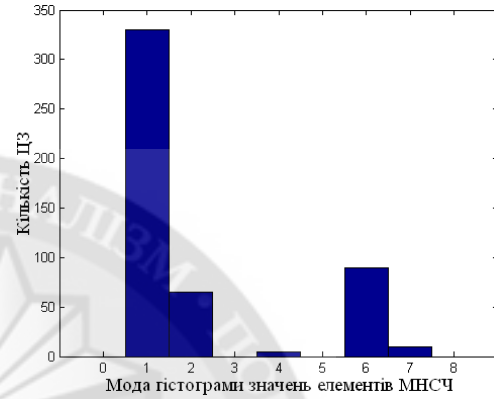
а



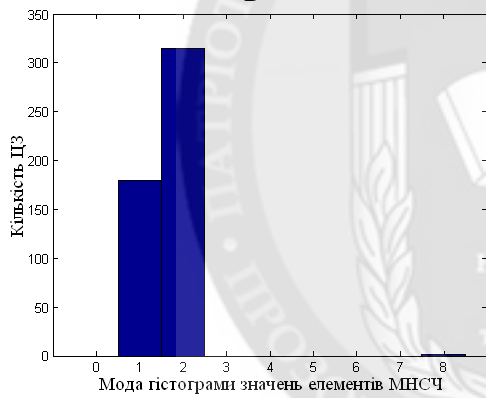
б



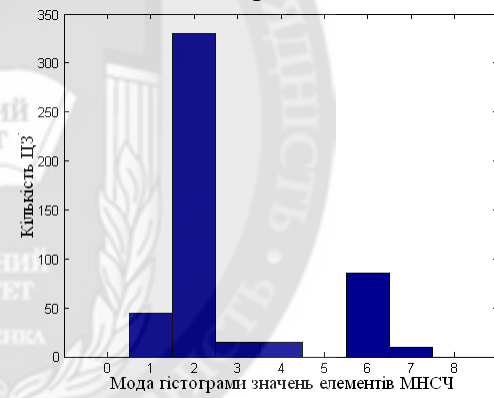
в



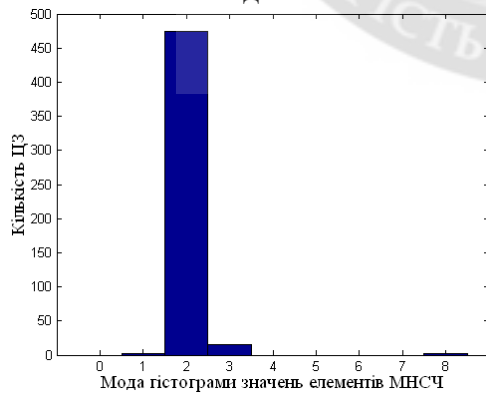
г



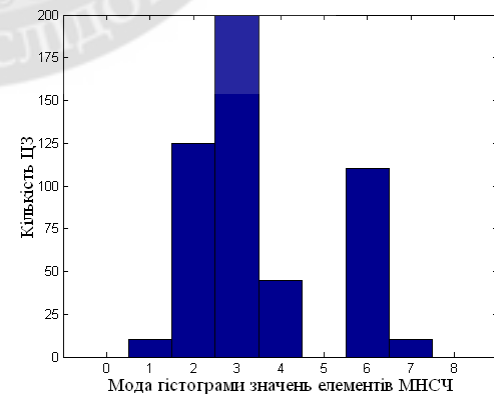
д



е



ж



з

Рисунок 3. Гістограми мод гістограм значень елементів МНСЧ блоків: а – $T = 0.1$ (множина Y); б – $T = 0.1$ (множина $Y^{(75)}$); в – $T = 0.3$ (множина Y); г – $T = 0.3$ (множина $Y^{(75)}$); д – $T = 0.5$ (Y); е – $T = 0.5$ ($Y^{(75)}$); ж – $T = 0.7$ (Y); з – $T = 0.7$ ($Y^{(75)}$)

Тут і далі при проведенні обчислювальних експериментів в роботі використовується множини:

Y , що містить 500 ЦЗ з загально використовуваної бази [21] в форматі без втрат (Tif);

$Y^{(70)}$, $Y^{(75)}$, $Y^{(80)}$ отримані шляхом Perezбереження ЦЗ з множини Y у формат с втратами

Jpeg з $QF \in \{70,75,80\}$ відповідно; $|Y^{(70)}| = |Y^{(75)}| = |Y^{(80)}| = 500$, де $|\cdot|$ – потужність множини.

Для експериментів ЦЗ обрізалися до розміру 800×800 пікселів.

Серед ЦЗ в форматі без втрат, які були задіяними при проведенні обчислювального експерименту, наявні такі (3 ЦЗ), що поводять себе як «виняток з правила» – саме їм відповідають стовпчики гістограм мод гістограм з аргументом 8 (рис.3(а,в,д,ж)). При детальному дослідженні цих ЦЗ стає зрозумілим, що їх поведінка цілком виправдана. Одне з таких ЦЗ для наочності наведене на рис.5. Блоки отриманого досліджуваного 800×800 ЦЗ в більшості своїй не містять ніяких деталей, частин контурів, тобто їх високочастотна складова майже відсутня ще до стиску; крім того, кожна кольорова складова ЦЗ (рис.5(в) – синя складова) має значну кількість блоків, елементи яких дорівнюють нулю чи є близькими до нуля, що приводить до того, що майже всі СНЧ блоку дорівнюють/порівнянні з нулем. Якщо збільшити розміри частини ЦЗ, що досліджується, то характер гістограми змінюється до «стандартного» для ЦК в форматі без втрат (рис.6), зміщуючи положення моди з 8 до 0. Дійсно, збільшення розміру частини, що досліджується, приводить до «підключення» блоків, високочастотна складова в яких не є порівняною з нулем, які містять наявні деталі, частини контурів. Але очевидно, що такий крок не завжди приведе до покращення результату. Дійсно, якщо ЦЗ/кадр ЦВ цілком є таким, перепади значень яскравості в якому є незначними, високочастотна складова навіть в форматі без втрат практично відсутня, то такий ЦК може мати більшість блоків, для яких кількість СНЧ, менших заданого параметра T , може бути значною, тобто характер гістограми значень елементів МНСЧ для ЦК в форматі без втрат буде мати властивості гістограми для випадку формату з втратами. І хоча на практиці кількість таких оригінальних контентів є дуже незначною, вони вимагають додаткового дослідження, результати якого виходять за межі даної статті і зараз готуються до друку.

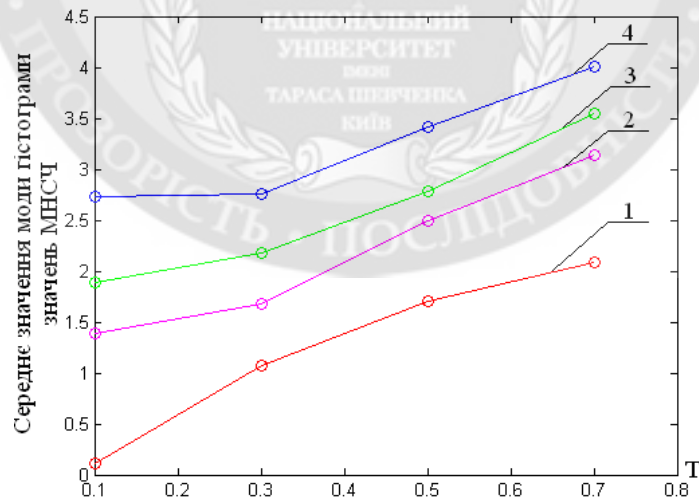


Рисунок 4. Графіки залежності середнього по експерименту значення моди гістограми значень елементів МНСЧ від параметру T : 1 – ЦЗ з множини Y ; 2, 3, 4 – відповідні ЦЗ з множин $Y^{(80)}$, $Y^{(75)}$, $Y^{(70)}$ відповідно

Аналіз гістограм мод гістограм значень елементів МНСЧ (рис.3), а також середніх значень моди гістограми МНСЧ (рис.4) дає можливість визначитися з найбільш пріоритетним

серед розглянутих значенням параметра $T \in \{0.1, 0.3, 0.5, 0.7\}$. Це значення $T = 0.1$, що впливає з урахуванням наступного:

Для $T = 0.1$ має місце найбільша відмінність значень мод гістограм елементів МНСЧ блоків для цифрових контентів в різних (з/без втрат) форматах;

Для конкретного ЦЗ/кадру ЦВ для будь-якого значення (10) T можлива ситуація, коли моди гістограм значень елементів МНСЧ відповідних цифрових контентів будуть співпадати. Для $T = 0.1$ така ситуація буде мати місце рідше за інші значення параметра (рис.3);

Найменше з використаних значень параметру $T = 0.1$, враховуючи нечутливість СНЧ, зокрема найменших за значенням, відповідно з (4), дозволяє виявити в блоці кількість саме таких СНЧ, які в результаті квантування і округлення частотних коефіцієнтів блоків в процесі стиску були нулями. А саме ці СНЧ і є тою основною ознакою, яка відрізняє ЦК в різних (з/без втрат) форматах.



Рисунок 5. Тестове ЦЗ: а – вхідне ЦЗ; б – досліджуване ЦЗ розміром 800×800 пікселів; в – синя складова досліджуваного ЦЗ

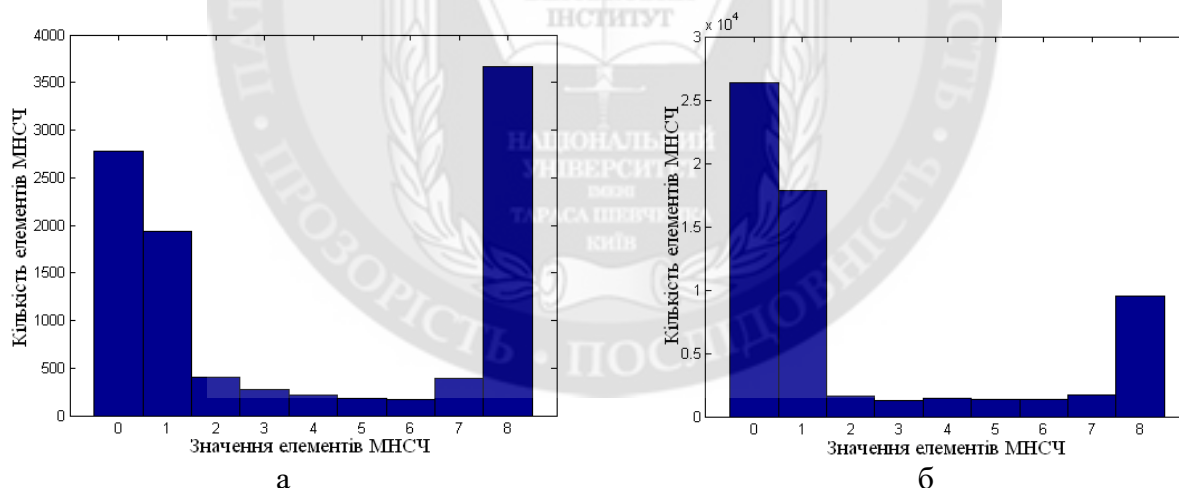


Рисунок 6. Гістограми тестового ЦЗ при зміні його розміру: а – 800×800 пікселів (рис.5(в)); б – 2000×2000 пікселів

З урахування отриманих результатів обчислювального експерименту (рис.3) очевидно є можливість співпадіння мод гістограм значень елементів МНСЧ блоків ЦК в різних (з/без втрат) форматах. При детальному дослідженні встановлено, що така ситуація має місце для ЦЗ/кадру ЦВ, сцена якого має велику кількість деталей, значних перепадів значень яскравості, тобто має значну високочастотну складову навіть при збереженні з втратами. Приклад такого ЦЗ проілюстрований на рис.7, гістограми значень елементів МНСЧ блоків для відповідних ЦЗ наведені на рис.8.



Рисунок 7. Тестове ЦЗ

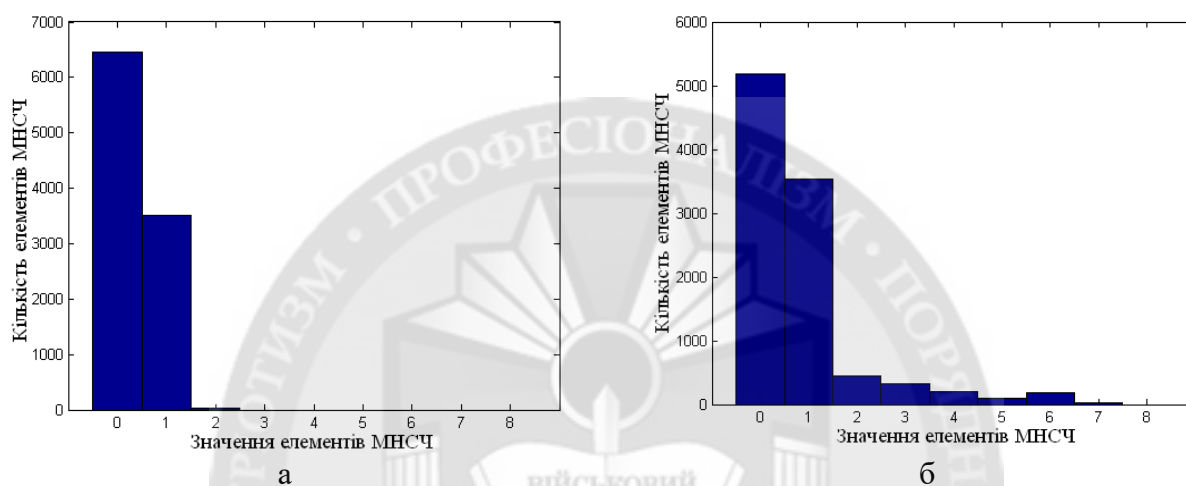


Рисунок 8. Ілюстрація відмінностей гістограм елементів МНСЧ ($T = 0.1$) відповідних ЦЗ у різних форматах збереження при співпадінні їх мод: а – ЦЗ в форматі без втрат (Tif) (рис.7); б – відповідне ЦЗ в форматі з втратами (Jpeg ($QF = 75$))

Наявність можливості співпадіння мод гістограм МНСЧ блоків для відповідних цифрових контентів вказує на недостатність використання лише одного параметру аналізованої гістограми – її моди для того, щоб відокремити контенти в різних форматах збереження. Але, як вже зазначалося вище, МНСЧ блоків для цифрових контентів в різних форматах збереження відрізняються своїм вмістом: значення елементів для ЦК в форматі з втратами є неменшими ніж у відповідних ЦК форматі без втрат, ілюстрацією чого є рис.1,2,8. З урахуванням цього висувається наступна гіпотеза: для переважної більшості оригінальних ЦК в форматі без втрат максимальне значення МНСЧ блоків є не більшим за відповідне значення для ЦК у форматі з втратами. Ця гіпотеза знайшла своє практичне підтвердження в результаті обчислювального експерименту (табл.1). Встановлено, що для 97% досліджених при проведенні обчислювального експерименту ЦЗ її висновок має місце.

Нехай розглядається задача встановлення формату послідовності ЦЗ (одного формату) чи ЦВ, збереженого у конкретному форматі. Тут відповідь на поставлене питання може бути отриманою за допомогою аналізу гістограми Γ_{DV} мод гістограм елементів МНСЧ блоків сукупності ЦЗ/кадрів ЦВ, враховуючі значні відмінності цих гістограм (порівн. рис.3(а) і 3(б), рис.3(в) і 3(г) і т.д.) для контентів в різних (з/без втрат) форматах після отримання кількісних оцінок цих відмінностей:

4. Мода гістограми значень елементів МНСЧ тим більше, чим менше значення коефіцієнта якості, що використовувався в процесі стиску контенту; для цифрових контентів в форматі без втрат значення моди не більше, ніж для контентів в форматі з втратами;

5. Визначене найбільш пріоритетне значення параметра T , що обмежує зверху значення СНЧ блоків матриці цифрового контенту, що задіюються в процесі його експертизи: $T = 0.1$, яке сприяє найбільшій різниці у властивостях відповідних МНСЧ блоків для контентів в різних форматах збереження;

6. Встановлено, що для 97% протестованих ЦЗ максимальне значення МНСЧ блоків для зображення в форматі з втратами є неменшим за відповідне значення відповідного ЦЗ у форматі без втрат;

7. Для послідовності ЦЗ одного формату, для ЦВ визначений формальний математичний об'єкт – гістограма мод гістограм МНСЧ блоків ЦЗ/кадрів ЦВ, властивості якої значно розрізняються для різних форматів збереження, що може бути використаним для розробки відповідного експертного методу.

8. Встановлення кількісних характеристик для отриманих в роботі якісних роздільників дасть можливість сформулювати ефективний метод відокремлення ЦК в різних форматах збереження, що може бути застосованим як складова частина процесу стеганоаналізу, в процесі виявлення результатів фотомонтажу, де були задіяні ЦК в різних форматах тощо, тобто націлений на підвищення ефективності виявлення порушення цілісності ЦК.

ЛІТЕРАТУРА

1. Rai, A., Singh, A.S., Kumar, A.S. A review of information security: issues and techniques / *International Journal for Research in Applied Science & Engineering Technology*. 2020. 8(5). P. 953–960.
2. Shwetha, B., Sathyanarayana, S.V. Digital image forgery detection techniques: a survey / *ACCENTS Transactions on Information Security*. 2017. 2(5). P. 22–31.
3. Alqahtani, F.H. Developing an information security policy: a case study approach / *Procedia Computer Science*. 2017. 124, P. 691–697.
4. Karthikeyan, N., Saravana Kumar, N.M., Mugunthan, S.R. Comparative study of lossy and lossless image compression techniques / *International Journal of Engineering & Technology*. 2018. 7. P. 950–953.
5. Гонсалес, Р., Вудс, Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
6. Taher, M.M., Ahmad, A.R., Hameed, R.S., Mokri, S.S. A literature review of various steganography methods / *Journal of Theoretical and Applied Information Technology*. 2022. 100(5). P. 1412–1427.
7. Aggarwal, A., Sangal, A., Varshney, A. Image steganography using LSB algorithm / *International Journal of Information Sciences and Application*. 2019. 11(1). P. 85–89.
8. Dhawan, S., Gupta, R. Analysis of various data security techniques of steganography: a survey / *Information Security Journal: A Global Perspective*. 2021. 30(2). P. 63–87.
9. Кобозева, А.А. Использование особенностей возмущений сингулярных чисел матрицы цифрового изображения для обнаружения его фальсификации / *Штучний інтелект*. 2008. 1. С. 145–153.
10. Jalab, H.A., Subramaniam, T., Ibrahim, R.W., Kahtan, H., Mohd Noor, N.F. New texture descriptor based on modified fractional entropy for digital image splicing forgery detection / *Entropy*. 2019. 21(4). 371.
11. Tjoa, S., Lin, W.S., Zhao, H.V., Liu, K.J.R. Block size forensic analysis in digital images / *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP 2007, April 15–20, 2007, Honolulu, Hawaii, USA*. P. I-633-I-636.
12. Luo, W., Huang, J., Qiu, G. A novel method for block size forensics based on morphological operations / *Digital Watermarking (IWDW 2008), Lecture Notes in Computer Science*. 2008. 5450. P. 229–239.
13. 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.
14. Akhmetieva, A.V. Method of detection the fact of compression in digital images as an integral part of steganalysis / *Інформатика та математичні методи в моделюванні*. 2016. 6(4). С. 357–364.
15. Бобок, І.І. Метод виявлення зображень, перезбережених у формат без втрат з формату з втратами / *Математичне та комп'ютерне моделювання*. 2017. 16. С. 5–14.

16. Кобозева, А.А., Хорошко, В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
17. 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.
18. 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.
19. Деммель, Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
20. Каханер, Д., Моулер, К., Нэш, С. Численные методы и программное обеспечение. М.: Мир, 2001. 573 с.
21. 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.

REFERENCES

1. Rai, A., Singh, A.S., Kumar, A.S. (2020), “A review of information security: issues and techniques”, *International Journal for Research in Applied Science & Engineering Technology*, 8(5), pp. 953–960.
2. Shwetha, B., Sathyanarayana, S.V. (2017), “Digital image forgery detection techniques: a survey”, *ACCENTS Transactions on Information Security*, 2(5), pp. 22–31.
3. Alqahtani, F.H. (2017), “Developing an information security policy: a case study approach”, *Procedia Computer Science*, 124, pp. 691–697.
4. Karthikeyan, N., Saravana Kumar, N.M., Mugunthan, S.R. (2018), “Comparative study of lossy and lossless image compression techniques”, *International Journal of Engineering & Technology*, 7, pp. 950–953.
5. Gonzalez, R.C., Woods, R.E. (2006), “*Tsifrovaya obrabotka izobrazheniy*” [Digital Image Processing], Technosfera, Moscow, 1070 p.
6. Taher, M.M., Ahmad, A.R., Hameed, R.S., Mokri, S.S. (2022), “A literature review of various steganography methods”, *Journal of Theoretical and Applied Information Technology*, 100(5), pp. 1412–1427.
7. Aggarwal, A., Sangal, A., Varshney, A. (2019), “Image steganography using LSB algorithm”, *International Journal of Information Sciences and Application*, 11(1), pp. 85–89.
8. Dhawan, S., Gupta, R. (2021), “Analysis of various data security techniques of steganography: a survey”, *Information Security Journal: A Global Perspective*, 30(2), pp. 63–87.
9. Kobozeva, A.A. (2008), “Ispol’zovanie osobennostey vozmuscheniy singulyarnykh chisel matritsi tsifrovogo izobrazheniya dlya obnaruzheniya ego fal’sifikatsii” [Application of image matrix singular values disturbances for image forgery detection], *Artificial Intelligence*, 1, pp. 145–153.
10. Jalab, H.A., Subramaniam, T., Ibrahim, R.W., Kahtan, H., Mohd Noor, N.F. (2019), “New texture descriptor based on modified fractional entropy for digital image splicing forgery detection”, *Entropy*, 21(4), 371.
11. Tjoa, S., Lin, W.S., Zhao, H.V., Liu, K.J.R. (2007), “Block size forensic analysis in digital images”, *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP 2007*, April 15–20, 2007, Honolulu, Hawaii, USA. pp. I-633–I-636.
12. Luo, W., Huang, J., Qiu, G. (2008), “A novel method for block size forensics based on morphological operations”, *Digital Watermarking (IWDW 2008), Lecture Notes in Computer Science*, 5450, pp. 229–239.
13. 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.
14. Akhmetieva A.V. (2016), “Method of detection the fact of compression in digital images as an integral part of steganalysis”, *Informatics and mathematical methods in modelling*, 6(4), pp. 357–364.
15. Bobok, I.I. (2017), “Metod vyyavlennyyazobrazhen’, perezberezhnyy u format bez vtrat z formatu z vtratamy” [A method for detecting images converted to a lossless format from a lossy format], *Mathematical and Computer Modelling. Series: Technical Sciences*, 16, pp. 5–14.
16. Kobozeva, A.A., Khoroshko, V.A. (2009), “*Analiz informatsionnoy bezopasnosti*” [Information Security Analysis], GUIKT, Kyiv, 251 p.
17. Bobok, I.I. (2017), “Rozvytok zagalnogo pidhodu do problem vyyavlennya porushen’ tsilisnosti tsyfrovyyh 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.

18. 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.
19. Demmel, D. (2001), “*Vychislitel'naya linejnaya algebra: teoriya i prilozheniya*” [Numerical Linear Algebra: Theory and Applications], Mir, Moscow, 430 p.
20. Kahaner, D., Moler, C., Nash, S. (2001), “*Chislennye metody i programmnoe obespechenie*” [Numerical Methods and Software], Mir, Moscow, 573 p.
21. Gloe, T., Böhme, R. (2010), “The “Dresden Image Database” for benchmarking digital image forensics”, *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC '10)*, pp. 1585–1591.

D.Sci. Bobok I.I., D.Sci. prof. Kobozieva A. A., D.Sci. prof. Maevsky D.

STUDY OF THE PARAMETERS OF THE DIGITAL CONTENT MATRIX BLOCKS IN DIFFERENT STORAGE FORMATS AS A THEORETICAL BASIS FOR THE METHODS OF DETECTING VIOLATIONS OF ITS INTEGRITY

Unauthorized changes of digital information contents, in particular images, videos, which are considered in the work, the detection of which is a difficult and urgent task, require the development of new approaches and methods. In case of unauthorized changes in digital contents, there is often a change in the format (lossy/lossless) of its preservation (in whole or in part), in particular when organizing a steganographic communication channel, photomontage, etc. Thus, the identification of the fact of re-preservation of digital content in a format different from the original one is a pointer to the violation of its integrity, making the task of separating content in different formats urgent. The aim of the work is to study the properties of the formal parameters of blocks of original digital content to create a theoretical basis for the methods of separating content in various storage formats. In the course of the study: the formal parameters – the smallest singular values of the blocks of the corresponding matrices, based on the properties of which the proposal to introduce a formal research object – the matrix of the smallest singular values of the blocks, corresponding to the digital content and having properties that differ depending on from the digital content storage format – were determined; for a sequence of digital images of the same format, for digital video, a formal mathematical object is defined – a histogram of modes of histograms of matrices of the smallest singular values of blocks of images/frames of video, the properties of which differ significantly for different storage formats, which can be used to develop an appropriate expert method. Establishing quantitative characteristics for qualitative separators obtained in the work will provide an opportunity to form effective methods of separating digital contents in various storage formats, which can be applied as a component of the steganalysis process, in the process of detecting the results of photomontage, where contents in various formats were involved, etc.

Keywords: digital image, digital video, lossy format, lossless format, singular value