тод дозволяє вирішити проблему накопичення обчислень, що, в свою чергу, приводить алгоритм чисельної реалізації до такого вигляду, при якому можливе отримання розв'язків в режимі реального часу. Отримані інтегральні моделі володіють достатнім рівнем адекватності та можуть використовуватись в інтегрованих обчислювальних системах керування об'єктів енергетичного призначення.

Ключові слова: *інтегральні моделі, вироджене ядро, ідентифікація моделі, контроль результатів ідентифікації.*

Отримано: 10.10.2022

УДК 004.056.5
DOI: 10.32626/2308-5916.2022-23.55-72

А. А. Кобозєва, д-р техн. наук,
Д. А. Маєвський, д-р техн. наук,
О. М. Симонова

Національний університет «Одеська політехніка», м. Одеса

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ КОЕФІЦІЄНТІВ ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ ЯК ОСНОВА МЕТОДА ВИЯВЛЕННЯ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

Одним з найпоширеніших представлень інформації сьогодні є цифрові зображення (ЦЗ), несанкціоновані зміни яких можуть приводити до негативних наслідків як для окремої людини, установи, фірми, так і для держави в цілому, що робить задачу виявлення порушення цілісності ЦЗ одною з найактуальніших задач інформаційної безпеки. Основним недоліком існуючих експертних методів є їх орієнтованість на виявлення результатів конкретної збурної дії, але на практиці експерт часто не володіє інформацію про конкретику атаки на ЦЗ, при цьому набір його засобів завжди є обмеженим, що може привести до ситуації, коли досліджуване ЦЗ помилково бути визнане оригінальним. Першим «ешелоном оборони» тут повинні бути методи, ефективні незалежно від виду збурної дії — універсальні. На теперішній час в відкритих джерелах представлена дуже незначна кількість таких методів, які не є вільними від недоліків, головним з яких є суттєве зниження ефективності в умовах незначних збурних дій. Метою роботи є розробка теоретичного базису для ефективного універсального методу виявлення порушення цілісності ЦЗ, зокрема, в умовах незначної збурної дії. В ході досягнення мети в роботі: обґрунтована доцільність використання блокового підходу при організації експертизи цілісності ЦЗ; область дискретного косинусного перетворення (ДКП) блоку обрана як область

проведення експертизи; обгрунтований вибір конкретних коефіцієнтів ДКП для організації виявлення порушення цілісності ЦЗ, значення яких не залежать від значення коефіцієнту якості, що використовувався при отриманні оригінального зображення, а також від конкретного виду ЦЗ; досліджено відмінність в характері змін обраних формальних параметрів при перезбереженні ЦЗ з втратами залежно від того, оригінальним чи неоригінальним воно є. Отримані результати теоретичних досліджень, що підтверджуються результатами обчислювальних експериментів, складають теоретичний базис для розробки ефективного універсального методу експертизи цілісності ЦЗ, зокрема, в умовах незначної збурної дії.

Ключові слова: *цифрове зображення, порушення цілісності зображення, дискретне косинусне перетворення, блокова обробка, формат збереження з втратами.*

Вступ. Цифрові зображення (ЦЗ) разом з цифровим відео на сьогодні є одним з найпоширеніших представлень інформації, для якої її цілісність є одним з критеріїв захищеності [1]. Несвоєчасне виявлення чи взагалі невиявлення порушення цілісності ЦЗ може приводити до негативних наслідків як для окремої людини, установи, фірми, так і для держави в цілому, якщо неавторизовані підробки використовуються як речові докази в судових розслідуваннях, в засобах масової інформації для дискредитації, «чорного» піару окремих політичних діячів, неправдивого подання важливих світових подій тощо, що дуже активно застосовується при ведені сучасних інформаційних та гібридних війн, де «інформаційний простір стає сферою і середовищем боротьби, аналогічним суші, воді, повітрю, політиці, економіці тощо» [2], і що ми спостерігаємо зараз у вигляді значних, хоча і безуспішних для світової спільноти, «потуг» російської пропаганди при повномасштабному вторгненні в Україну РФ: численні підробки, фейки, неправдива інформація на різних рівнях поширюються Росією в світі з метою компрометації України [3]. Все це робить задачу виявлення порушення цілісності інформаційних контентів, зокрема ЦЗ, одною з найактуальніших сучасних задач інформаційної безпеки.

Всі методи виявлення порушення цілісності ЦЗ можна розбити на дві великі групи: активні і пасивні (або «сліпі») відповідно до того, потрібна чи не потрібна інформація про оригінальне ЦЗ для його експертизи [4]. Активні методи забезпечують перевірку порушення/непорушення цілісності контенту, використовуючи для цього електронний цифровий підпис або техніку цифрових водяних знаків, при цьому кожний з варіантів має значні недоліки. Дійсно, при використанні електронного цифрового підпису є потенційна можливість його компрометації, алгоритм його формування складний в обчислювальному сенсі і є порівняно пові-

льним навіть при незначній довжині ключа, необхідною є організація інфраструктури відкритого ключа в кожній з організацій-користувачів технології електронних цифрових підписів. Що стосується другого варіанту, то, на думку авторів, він взагалі є принципово неприйнятним в умовах задачі, що розглядається, оскільки вбудова цифрового водяного знаку в ЦЗ сама по собі порушує його цілісність. Все це привело до того, що останнім часом перевага надається саме пасивним методам [4, 5], ідея розробки яких є основною і в даній роботі.

Пасивні методи виявлення порушень цілісності ЦЗ можна розділити на наступні групи [4, 6]: піксель-орієнтовані (*pixel-based*), орієнтовані на області перетворення ЦЗ (детектують «аномалії» у значеннях яскравості пікселів ЦЗ чи формальних параметрів в областях перетворення зображення); формат-орієнтовані (*format based*) (детектують порушення цілісності шляхом аналізу артефактів, що виникають при стиску ЦЗ); камера-орієнтовані (*camera based*) (використовують технічні характеристики камери для детектування слідів несанкціонованих змін ЦЗ); орієнтовані на фізичне навколишнє середовище (*physical environment based*) (засновані на оцінці й зіставленні освітленості об'єктів на ЦЗ); орієнтовані на геометрію зображення (*geometry based*) (засновані на виявленні неточностей при порівнянні геометричних особливостей і характеристик об'єктів у реальності й на ЦЗ). Така класифікація вказує на специфіку роботи методів, на область їх пріоритетної «уваги», що очевидно є й покажчиком на відносну обмеженість області їх застосування, зокрема: при відсутності даних про технічні характеристики камери, на якій було отримане досліджуване ЦЗ, що на практиці має місце досить часто, відповідний метод стає недієздатним; орієнтованість на фізичне навколишнє середовище не спрацює у випадку затемненого ЦЗ тощо. Взагалі більшість існуючих «сліпих» методів має обмежену область застосування: орієнтованість на конкретний формат, у якому збережені досліджувані ЦЗ [7, 8], на величину збурення, що зазнає оригінальний контент, яка є формальним представленням порушення його цілісності (багато методів є неспроможними виявити результати незначної збурної дії) [9] і т.і. Але основним недоліком переважної більшості існуючих методів є їх орієнтованість на конкретну (конкретні) збурну дію (дії), відповідно до особливостей якої будуються і їх математичні базиси. Так метод, запропонований в [10], налаштований на виявлення штучного підвищення різкості ЦЗ, методи [11, 12] — на результати розмиття ЦЗ чи його частини; розробка, запропонована в [13], розрахована на виявлення зміни яскравості; методи [14, 15] виявляють накладання шуму.

Враховуючи те, що стеганоперетворення ЦЗ-контейнера на практиці теж приводить до його зміни, то до пасивних методів вияв-

лення порушень цілісності можна по праву віднести і стеганоаналітичні методи, основною задачею яких є саме виявлення факту наявності додаткової інформації в контенті. Більшість стеганоаналітичних методів також є спрямованими на виявлення результатів конкретних стеганоалгоритмів або ж навіть їх конкретних реалізацій [16-18].

Необхідно зазначити, що на практиці експерт дуже часто не володіє інформацію про конкретику збурної дії, яка, можливо, була застосована до інформаційного контенту, при цьому набір засобів, програмно реалізованих методів, що є у розпорядженні експерта, завжди є скінченим. І якщо цей набір містить лише спрямовані методи, а серед них немає такого, який розрахований на застосовану збурну дію, то досліджуване ЦЗ може помилково бути прийнятим за оригінальне з усіма негативними наслідками, які з цього випливають. Єдиним можливим виходом тут є застосування універсальних експертних методів — «першого ешелону оборони», які зберігають свою дієздатність незалежно від того, якій саме збурній дії піддалося ЦЗ.

Побудова універсального методу потребує створення для нього такого математичного базису, який би не був залежним від специфіки збурної дії. Цей математичний базис повинен відрізняти оригінальне ЦЗ від неоригінального при будь-яких порушеннях цілісності, бути налаштованим на виявлення відмінностей властивостей формальних параметрів ЦЗ, цілісність якого порушена, від властивостей параметрів оригінального ЦЗ. На сьогодні існує незначна кількість таких методів, інформація про які є доступною з відкритих джерел, що пояснюється, в першу чергу, складністю самої задачі їх побудови. Прикладами універсальних методів є розробки, представлені в [19, 20]. Тут «універсальний» математичний базис, розроблений попередньо в [21], заснований на аналізі нормованого вектора сингулярних чисел (СНЧ) і лівого і правого сингулярних векторів (СНВ), що відповідають найбільшому сингулярному числу, блоків матриці ЦЗ, отриманих шляхом її стандартної розбивки. Кожен з цих методів є ефективним, незалежно від виду збурної дії, але ефективність їх значно знижується із зменшенням сили збурної дії, що обмежує область їх застосування, є недоліком.

Таким чином, задача виявлення порушення цілісності ЦЗ не має на цей час остаточного задовільного розв'язку, зокрема розробка нових, удосконалення існуючих універсальних експертних методів, що зберігають ефективність в умовах незначної збурної дії, залишається актуальною задачею інформаційної безпеки, потребує для свого розв'язку розробки нових теоретичних підходів.

Мета та задачі дослідження. *Метою* роботи є розробка теоретичного базису для наступного створення на його основі ефективного пасивного універсального методу виявлення порушення цілісності ЦЗ, зокрема, в умовах незначної збурної дії.

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

1. Обґрунтувати вибір області ЦЗ для проведення експертизи його цілісності;
2. Обґрунтувати в обраній області ЦЗ вибір конкретних параметрів, аналіз яких має сенс використовувати для експертизи його цілісності; перевірити експериментально доцільність аналізу обраних параметрів для розв'язку задачі, що розглядається.

Викладення основного матеріалу дослідження. Не обмежуючи спільності міркувань, будемо вважати, що формальним представленням ЦЗ є одна $n \times n$-матриця F. Результат порушення цілісності ЦЗ можна представити в загальному вигляді як збурення його матриці [22]:

$$\overline{F} = F + \Delta F \ , \qquad (1)$$

де $\overline{F}$ — $n \times n$-матриця ЦЗ, цілісність якого порушена, ΔF — $n \times n$-матриця, що є формальним представленням збурної дії.

Тоді, з урахуванням (1), виявлення порушення цілісності буде означати в загальному сенсі встановлення, що

$$\overline{F} \neq F \ , \qquad (2)$$

при цьому для «сліпого» методу висновок (2) повинен бути зроблений без наявності інформації про оригінальне ЦЗ з матрицею F, що значно ускладнює задачу в порівнянні з активним методом, особливо в умовах незначної ΔF .

Ефективність будь-якого універсального методу, яка для експертних методів, як правило, визначається точністю виявлення порушення цілісності [23] (*accuracy* (*ACC*)) та обчислюється у відповідності до формули:

$$ACC = \left(TP + TN\right) \Big/ \left(TP + FN + TN + FP\right), \qquad (3)$$

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, в умовах конкретної збурної дії буде очевидно невищою, а на практиці — нижчою за ефективність спрямованого методу, який на цю збурну дію розрахований і при своїй реалізації налаштований на врахування особливостей саме цієї конкретної збурної дії [19]. Очікуваним, з урахуванням (1), також є зниження ефективності будь-якого експертного методу, зокрема універсального, зі зменшенням величини збурної дії: чим менше збурна дія, тим в загальному випадку більше ймовірність того, що відбиток її результату на аналізованих параметрах ЦЗ може бути невиявленим. І

хоча таке зниження ефективності є природнім, кількісно його результат може бути різним.

Єдиним способом для виявлення результату незначної збурної дії ΔF залишається використання при експертизі чутливих до збурних дій формальних параметрів матриці ЦЗ. При цьому найбільш доцільним тут є задіювання для експертизи області перетворення ЦЗ, що й робиться нижче. Дійсно, якщо мова буде йти про малу збурну дію, то помітити її результати в просторовій області, де всі пікселі по своїх властивостях є «рівноправними», де не існує на сьогодні можливості їх розподілу на чутливі та нечутливі до збурних дій, не маючи оригінального ЦЗ, може бути нерозв'язною задачею (наприклад, виявлення стеганоканалу, сформованого методом модифікації найменшого значущого біта (LSB) [17] з незначною пропускною спроможністю прихованого каналу зв'язку (ПСПК)). В той же час, в області перетворення ЦЗ (сингулярного, спектрального розкладання відповідної матриці, частотній області) зміни, що відбулися, є більш помітними при аналізі чутливих до збурних дій параметрів зображення, а виявлення таких параметрів не представляє труднощів.

З урахуванням (1), результат будь-якої збурної дії на ЦЗ з матрицею F можна представити у вигляді сукупності збурень СНЧ і СНВ матриці, отриманих за допомогою нормального сингулярного розкладання [22], яке є таким, що однозначно визначається для будь-якої матриці, що не має кратних СНЧ. На цьому засновані теоретичні базиси універсальних методів [19, 20]. Покажемо, що ефективність експертизи цілісності ЦЗ може бути збільшена шляхом перенесення її з області сингулярного розкладання матриці в частотну область, зокрема, враховуючи поширення для збереження і передачі ЦЗ формату з втратами Jpeg, в область дискретного косинусного перетворення (ДКП), яку використовує Jpeg. Дійсно, якщо переважна більшість ЦЗ зазнає при створенні обробку саме цим алгоритмом, то має сенс орієнтуватися на властивості результату такої обробки як на властивості оригінального ЦЗ.

Переважна більшість сучасних методів, що працюють з ЦЗ, зокрема Jpeg, є блоковими, тобто передбачають попередню розбивку матриці на блоки, частіше за все, будуючи її стандартну розбивку [24], з наступною обробкою окремих блоків. Це дає можливість забезпечити для будь-якого блокового методу при роботі з $n \times n$-матрицею порівняно незначну обчислювальну складність, що визначається кількістю блоків, і становить $O\left(n^2\right)$ операцій при послідовній алгоритмічній реалізації або розпаралелити процес, що є дуже актуальним при експертизах, що відбуваються в режимі реального часу, зокрема цифрового відео. Зважаючи на це, в роботі використовується блоковий підхід.

Нехай матриця F ЦЗ розбивається стандартним чином на $l \times l$-блоки, при цьому довільний з отриманих блоків позначимо B. Для B можливо побудувати нормальне сингулярне розкладання [25] у вигляді: $B = U\Sigma V^T$, 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 додатково є лексикографічно додатними; $\Sigma = diag\left(\sigma_1, ..., \sigma_l\right)$, $\sigma_1 \geq ... \geq \sigma_l \geq 0$ — СНЧ B. Сингулярне розкладання може бути також представленим у формі зовнішніх добутків [26]: $B = \sum_{i=1}^{l} \sigma_i u_i v_i^T$, де матриця B розкладається на суму одноранговых матриць $\sigma_i u_i v_i^T$, $i = \overline{1,l}$, кожна з яких визначається своєю сингулярною трійкою $\left(\sigma_i, u_i, v_i\right)$. Між сингулярними трійками $\left(\sigma_i, u_i, v_i\right)$, $i = \overline{1,l}$, матриці B та її частотними складовими існує певний зв'язок [22]: трійки $\left(\sigma_i, u_i, v_i\right)$ (матриці $\sigma_i u_i v_i^T$), які відповідають найбільшим сингулярним числам, несуть в собі, в основному, інформацію про низькочастотну складову сигналу, а ті, що відповідають найменшим СНЧ — в основному, про високочастотну складову. При цьому інформація про частотні складові, в більшій або меншій мірі, «розмазана» по всіх сингулярних трійках, не даючи можливості визначити чітко в області сингулярного розкладання формальне представлення кожної частотної складової. Для виявлення порушення цілісності ЦЗ в результаті збурної дії, зокрема незначної, як вже зазначалося вище, експертизі доцільно піддавати параметри, що є чутливими до збурних дій, тобто такі, збурення яких в результаті незначної збурної дії буде порівняно значним. В методах [19], [20] параметри, що аналізуються (нормований вектор СНЧ, лівий і правий СНВ, що відповідають максимальному СНЧ блоку), такій вимозі не задовольняють, що очевидно є причиною зниження їх ефективності в умовах незначних збурних дій. В блоках матриці найбільш чутливими до збурних дій у відповідності з формулою $\sin\theta_i \leq \frac{2\left\|\Delta B\right\|_2}{gap\left(i, B\right)}$, де ΔB — $l \times l$-матриця збурення блоку B, $\left\|\cdot\right\|_2$ – спектральна матрична норма [26], θ_i — гострий кут між СНВ u_i і $\overline{u}_i$, що відповідають i-му СНЧ в матрицях B і $B + \Delta B$ відповідно, $gap\left(i, B\right) = \min_{j \neq i}\left|\sigma_i - \sigma_j\right|$ —

відокремленість СНЧ σ_i, будуть такі СНВ, що відповідають СНЧ з малими відокремленостями, а для блоку ЦЗ — це є найменші СНЧ. Враховуючи, що в (блоці) матриці ЦЗ сингулярні вектори, що відповідають найменшим СНЧ, будуть чутливими до збурних дій [22], чутливими будуть і відповідні матриці $\sigma_i u_i v_i^T$, приводячи до чутливості високочастотних коефіцієнтів (блоку) матриці ЦЗ. Використання безпосередньо високочастотних коефіцієнтів ДКП для експертизи цілісності зображення є більш доцільним, ніж використання $\left(\sigma_i, u_i, v_i\right)$ або матриці $\sigma_i u_i v_i^T$, оскільки в цій матриці присутні як середньо-, так і низькочастотні складові, які будуть «змазувати» потрібну картину зміни високочастотної складової.

Таким чином, як область проведення експертизи цілісності обирається частотна область блоків ЦЗ, а саме область ДКП; як параметри, що будуть піддаватися безпосередньому аналізу — чутливі до збурних дій високочастотні коефіцієнти ДКП блоків, що дасть можливість забезпечити ефективність експертизи цілісності ЦЗ, зокрема в умовах малої збурної дії.

Як оригінальні далі розглядаються ЦЗ в форматі Jpeg. Кожний блок *B* ЦЗ має декілька високочастотних коефіцієнтів, які чітко визначені в блоці коефіцієнтів ДКП (рис. 1). Оберемо той (ті) з них, які має сенс аналізувати при експертизі цілісності ЦЗ. При цьому до таких коефіцієнтів з урахуванням задачі, що розглядається, висуваються наступні вимоги:

- незалежність/незначна залежність від коефіцієнту якості *QF*, що використовувався при отриманні оригінального ЦЗ, які найчастіше застосовуються на практиці і далі називаються практично актуальними: $QF \in \{65, 75, 85\}$;
- незалежність/незначна залежність від конкретного ЦЗ ($QF \in \{65, 75, 85\}$).

Забезпечення висунутим вимогам, враховуючи відмінності в матрицях квантування [24] для різних значень коефіцієнту якості, можна з великою ймовірністю очікувати лише для коефіцієнтів ДКП (8,8), (7,8), (8,7) (рис. 1), оскільки для переважної більшості блоків будь-якого ЦЗ і будь-якого *QF* ці коефіцієнти обнуляються в результаті квантування і округлення, що відбувається в процесі стиску з втратами, і для відновленого після стиску довільного ЦЗ будуть порівнянні між собою та з похибкою округлення. Для вибору серед окремих коефіцієнтів ДКП (8,8), (7,8), (8,7), а також варіанту їх сукупного

врахування був проведений обчислювальний експеримент, в якому було задіяно 740 оригінальних ЦЗ (множина M_1), збережених з практично актуальними *QF*, що обиралися з традиційно використовуваних баз ЦЗ [27,28], а також зображення, отримані непрофесійними відеокамерами. Результати експерименту представлені в табл.1, де значення коефіцієнтів ДКП визначалися за модулем, оскільки передбаченим для врахування при експертизі цілісності є ступінь їх відміни від нуля; при цьому для суми абсолютних значень коефіцієнтів ДКП (8,8), (7,8), (8,7) використане позначення *S*.

Розкид середніх абсолютних значень для коефіцієнта ДКП (8,8), який є порівняним з розкидом для модулів коефіцієнтів (7,8) та (8.7), при $QF \in \{65, 75, 85\}$ складає 10.8%, при тому, як для суми абсолютних значень коефіцієнтів (8,8), (7,8), (8,7) — 28%, що вже говорить на користь використання одного з коефіцієнтів ДКП. Крім того, така ситуація має місце не тільки з згаданими середніми по експерименту значеннями, а й з значеннями для окремих ЦЗ, ілюстрація чого приведена на рис.2: швидкість зростання модулів коефіцієнтів ДКП (8,8), (7,8) (аналогічно поводе себе і коефіцієнт (8,7)) при зростанні *QF* значно менше ніж швидкість зростання суми модулів коефіцієнтів (8,8), (7,8), (8,7). При цьому, як показує обчислювальний експеримент, ця швидкість для коефіцієнта (8,8) буде найменшою для переважної більшості ЦЗ, що сприяє кращому задоволенню вимог, висунутих вище для коефіцієнтів ДКП, серед розглянутих. Таким чином, як формальний параметр, що буде аналізуватися в процесі експертизи цілісності ЦЗ, обирається коефіцієнт ДКП (8,8) 8×8-блоків зображення.

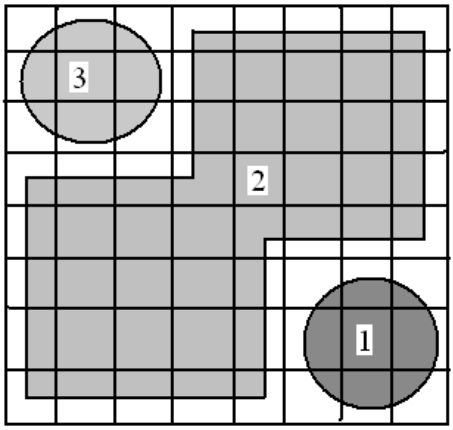


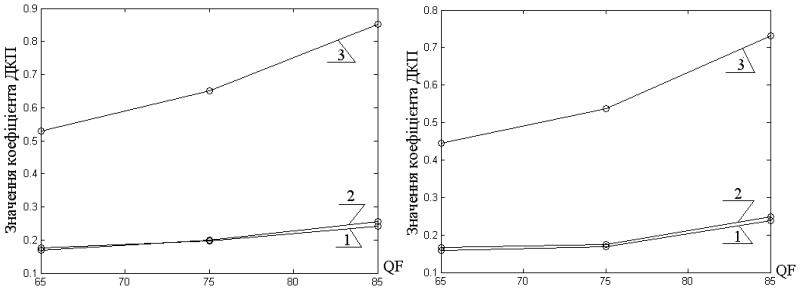
Рис. 1. *Розподіл частотних складових в матриці коефіцієнтів ДКП: 1 — високочастотні; 2 — середньочастотні; 3 — низькочастотні*

Таблиця 1

Значення високочастотних коефіцієнтів 8×8-блоків оригінальних ЦЗ, збережених в форматі Jpeg з практично актуальними значеннями коефіцієнта якості

Коефіцієнт(и) ДКП	Середнє значення			Мінімальне значення			Максимальне значення		
	QF			*QF*			*QF*		
	85	**75**	**65**	**85**	**75**	**65**	**85**	**75**	**65**
(8,8)	0.2423	0.2228	0.2162	0.1039	0.0546	0.0211	0.4886	0.4298	0.4291
(7,8)	0.2592	0.2170	0.2185	0.0959	0.0386	0.0110	0.4592	0.4156	0.4167
S	0.8612	0.6840	0.6198	0.3225	0.1412	0.0483	1.8484	1.5997	1.4527

Зазначимо, що хоча значення коефіцієнта ДКП (8,8) для будь-якого оригінального ЦЗ в форматі з втратами є порівнянних з похибкою округлення, при внесенні змін в зображення відповідно до формули (1) це значення, враховуючи чутливість до збурних дій, буде значно змінюватися навіть при малій збурній дії ΔB, що приведе в переважній більшості до значного зростання модуля (8,8). Дійсно, враховуючи, що значення коефіцієнта ДКП (8,8) близько до нуля, його значні зміни з більшою ймовірністю збільшать його модуль, ніж ще більше наближать до нуля, при цьому, чим більше величина збурної дії, тим значніше збільшиться модуль коефіцієнта (8,8), що підтверджується результатами обчислювального експерименту, представленими в табл.2, на рис.3, а також проілюстрованими для декількох ЦЗ, що первісно зберігалися у форматі Jpeg з *QF* = 75, на рис.4 (в якості збурних дій використовувалися стеганоперетворення методом *LSB* з різною ПСПК, при цьому ПСПК=0 біт/піксель тут відповідає оригінальному ЦЗ).



а *б*

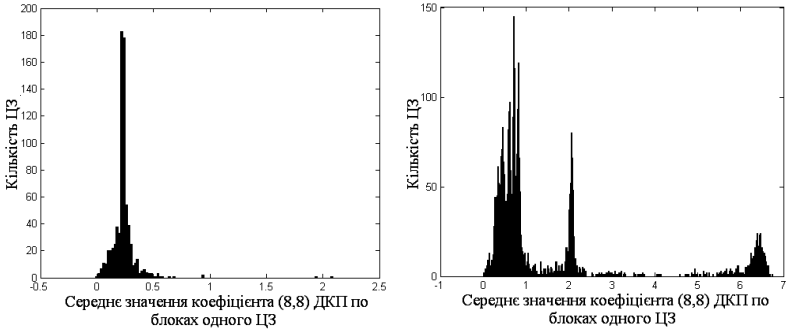
***Рис.2**. Графіки відповідності середніх значень модулів коефіцієнтів ДКП по 8×8-блокам матриці для двох (а,б) конкретних ЦЗ, обраних випадковим чином: 1 — коефіцієнт ДКП (8,8); 2 — коефіцієнт ДКП (7,8); 3 — S*

Таблиця 2

Середнє значення коефіцієнта ДКП (8,8) для 8×8-блоків оригінальних та збурених ЦЗ

Вид збурної дії	**Параметри збурної дії**	***PSNR* (*dB*)**	**Значення параметру *QF* оригінального ЦЗ в форматі Jpeg**		
			85	**75**	**65**
Збурна дія відсутня		–	**0.2423**	**0.2228**	**0.2162**
Гаусівський шум	D=0.00001	49.5	0.7557	0.7405	0.7311
	D=0.0001	40.5	2.0511	2.0452	2.0429
	D=0.001	31.5	6.1929	6.1819	6.1908
Мультиплікативний шум	D=0.00005	55.3	0.5359	0.5007	0.4905
	D=0.0001	51.8	0.6752	0.6461	0.6361
	D=0.001	41.6	1.7759	1.7618	1.7597
Стеганоперетворення методом *LSB*	ПСПК=1 біт/піксель	48.1	0.8491	0.8317	0.8257
	ПСПК=0.5 біт/піксель	51.1	0.6451	0.6250	0.6167
	ПСПК=0.25 біт/піксель	54.2	0.5055	0.4796	0.4724
	ПСПК=0.1 біт/піксель	58.1	0.3912	0.3583	0.3482

В експерименті було задіяно 740 оригінальних ЦЗ (множина M_1) та 3300 ЦЗ (множина M_2), цілісність яких була порушена з використанням різноманітних збурних дій, сила яких кількісно оцінювалася за допомогою різницевого показника спотворення ЦЗ в цілому *PSNR* — пікового відношення «сигнал-шум» [29]: $PSNR = \dfrac{n^2 \max\limits_{i,j} f_{ij}^2}{\left\|\Delta F\right\|_F^2}$, де $f_{ij}, i, j = \overline{1,n}$, — елементи матриці F, $\left\|\cdot\right\|_F$ – матрична норма Фробеніуса [26], та обиралася такою, що практично не порушує надійність сприйняття ЦЗ, яка встановлювалася за допомогою суб'єктивного ранжування (табл. 2).



а *б*

Рис. 3. *Гістограми значень коефіцієнтів ДКП (8,8): а — для оригінальних ЦЗ; б — для збурених ЦЗ*

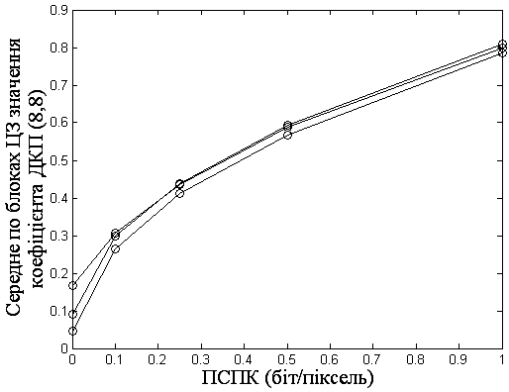
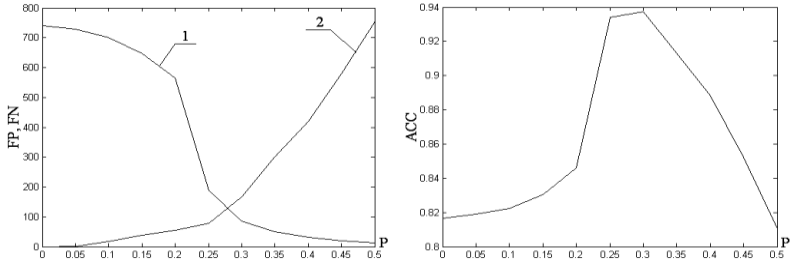


***Рис.4**. Зміна середнього по блоках ЦЗ абсолютного значення коефіцієнта ДКП (8,8) в залежності від пропускної спроможності прихованого каналу зв'язку*

Результати, представлені на рис. 3, вказують на можливість визначення порогового значення для величини коефіцієнта ДКП (8,8) для відокремлення оригінального ЦЗ від такого, цілісність якого порушена. Очевидно, що це порогове значення P повинно бути в межах [0, 0.5], де знаходиться переважна більшість оригінальних ЦЗ (рис. 3 (а)) і де є присутньою також значна кількість ЦЗ, цілісність яких порушена різноманітними збурними діями. Для кількісного визначення P було проведено обчислювальний експеримент, в якому були задіяні ЦЗ з множин M_1 і M_2. Для кожного значення $P \in [0, 0.5]$ з кроком 0.05 для ЦЗ з множини M_1 визначалися значення *TN, FP* (помилка другого роду), а для ЦЗ з множини M_2 — *TP, FN* (помилка першого роду), що використовуються в формулі (3), результати чого представлені на рис. 5 (а). Очевидно, що точка перетинання графіків залежності показників *FP, FN* від *P* є точкою відсікання [30], що визначає баланс між помилками першого та другого роду, незначний окіл якої може використовуватися як область, з якої обирається порогове значення *P*, що підтверджується відповідними результатами експерименту для значення *ACC* (3) (рис. 5(б)). Якщо в якості *P* взяти 0.28, то таке порогове значення дозволяє ефективно відокремлювати оригінальні і змінені ЦЗ навіть в умовах незначних збурних дій, що підтверджується обчислювальним експериментом і проілюстровано на рис.6: при експертизі ЦЗ, цілісність яких була порушена застосуванням в якості збурної дії стеганоперетворення *LSB*-методом з ПСПК = 0.25 біт/піксель (*PSNR* = 54.2 *dB*), помилок першого роду взагалі зафіксовано не було (рис. 6 (а)); при ПСПК = 0.1 біт/піксель (*PSNR* = 58.1 *dB*) помилки першого роду склали 8%.



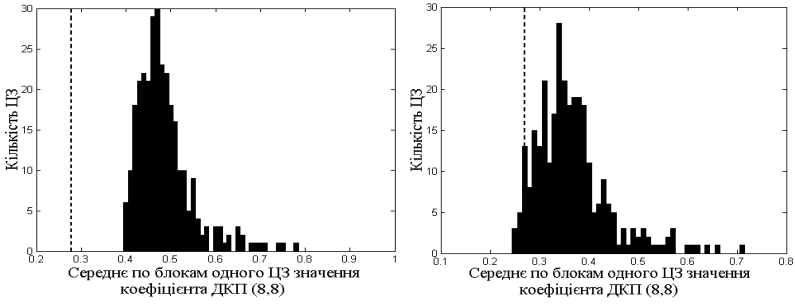
а *б*

***Рис. 5**. Визначення величини порогового значення P: а — графіки залежності показників FP, FN від P: 1 — FP; 2 — FN; б — графік залежності показника ACC від P*

Додатковою можливістю для підвищення ефективності використання коефіцієнтів ДКП блоків ЦЗ для експертизи його цілісності полягає в наступному. Нехай оригінальне ЦЗ, що збережене в форматі Jpeg з практично актуальним коефіцієнтом якості QF_1, перезберігається з значним коефіцієнтом $\overline{QF}$, для якого:

$$\overline{QF} > QF_1 . \qquad (4)$$

Після квантування і округлення при первісному збереженні (QF_1) коефіцієнт ДКП (8,8) блоку вже отримував нульове значення, яке після відновлення ЦЗ стало за модулем близьким до нуля, тому повторне квантування з матрицею квантування, елементи якої є меншими за відповідні елементи при первісному квантуванні, оскільки має місце співвідношення (4), приведе в результаті відновлення після повторного стиску лише до незменшення (на практиці — збільшення) коефіцієнта (8,8).



а *б*

***Рис. 6.** Результати обчислювального експерименту в умовах незначної збурної дії: а — гістограма для 300 ЦЗ з $QF \in \{65, 75, 85\}$, які використовувалися як контейнери для LSB-методу з ПСПК = 0.25 біт/піксель; б — ПСПК = 0.1 біт/піксель*

Припустимо тепер, що перезбереженню піддається ЦЗ, яке є результатом порушення цілісності оригінального зображення, що збе-

режене в форматі Jpeg з QF_1. Порушення цілісності оригінального ЦЗ приведе, як показано вище, до зростання модуля коефіцієнта ДКП (8,8) блоку у порівнянні з первісним значенням, ДКП (8,8) тепер відрізняється від нуля не лише завдяки операціям округлення, що відбуваються при відновленні ЦЗ після стиску, тут збільшення значення говорить про збільшення високочастотної складової в блоці зміненого зображення. Збереження ж такого зображення з втратами приводе до чергового зменшення високочастотної складової, тобто до зменшення модуля ДКП (8,8), що принципово відрізняє реакцію зміненого ЦЗ від оригінального на стиск з втратами. Для перевірки зробленого висновку був проведений обчислювальний експеримент, в якому аналізувалась R — відносна зміна значення модуля коефіцієнта ДКП (8,8) k_{88} в результаті перезбереження досліджуваного ЦЗ з $\overline{QF} = 100$:

$$R = \frac{\bar{k}_{88} - k_{88}}{k_{88}} \cdot 100\% \qquad (5)$$

де $\bar{k}_{88}$ — змінене значення k_{88}. Деякі з результатів експерименту в умовах незначних збурних дій, що в основному знаходяться у відповідності з отриманими вище теоретичними висновками, представлені на рис. 7.

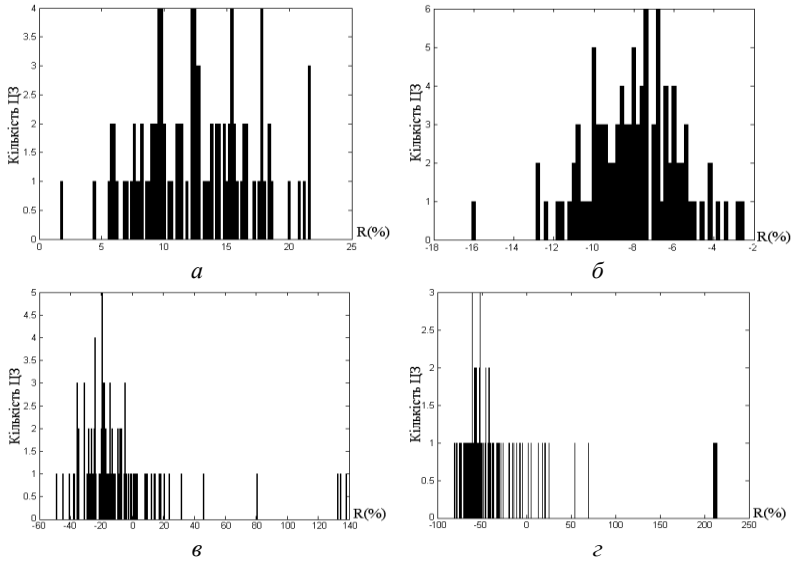


Рис. 7. *Гістограми значень R (5): а — при перезбереженні оригінальних ЦЗ (QF = 75); б — при перезбереженні ЦЗ (QF = 75), що піддалося накладанню гаусівського шуму D = 0.00001; в — при перезбереженні ЦЗ (QF = 75), що піддалося накладанню мультиплікативного шуму D = 0.00005; г — при перезбереженні ЦЗ (QF = 75), що піддалося накладанню мультиплікативного шуму D = 0.0001*

Запропонована додаткова перевірка характеру зміни модуля коефіцієнта ДКП (8,8) при перезбереженні досліджуваного ЦЗ в формат з втратами з $\overline{QF} = 100$ дозволила підвищити ефективність відокремлення ЦЗ в умовах незначної збурної дії, зокрема при виявленні результатів стеганоперетворення *LSB*-методом з ПСПК=0.1 біт/піксель помилки першого роду було зменшено до 6.5%, що говорить про підвищення ефективності у порівнянні з [19].

Висновки. В роботі розроблено теоретичний базис для організації пасивного виявлення порушення цілісності ЦЗ незалежно від конкретики збурної дії, якій піддалося зображення, в ході чого обґрунтовано:

- доцільність використання блокового підходу, який забезпечує порівняно незначну обчислювальну складність проведення експертизи, що становить $O\left(n^2\right)$ операцій для $n \times n$ -матриці ЦЗ;
- вибір області дискретного косинусного перетворення блоків матриці ЦЗ, отриманих в результаті її стандартної розбивки, яка дозволяє чітко виділити чутливі до збурних дій параметри блоку, для проведення експертизи цілісності;
- вибір конкретних параметрів, аналіз яких має сенс використовувати для експертизи цілісності ЦЗ — коефіцієнтів ДКП (8,8) блоків матриці ЦЗ, значення яких не залежать від значення практично актуальних коефіцієнтів якості *QF*, що використовуються при отриманні оригінального ЦЗ, а також від конкретного ЦЗ, що знайшло практичне підтвердження;
- відмінність в характері змін обраних для експертизи формальних параметрів при перезбереженні ЦЗ в формат з втратами залежно від того, оригінальним чи неоригінальним є зображення.

Отримані результати теоретичних досліджень, результати проведених обчислювальних експериментів, встановлена область значення порогу *P* для модуля коефіцієнтів ДКП (8,8) для відокремлення оригінальних ЦЗ від тих, що зазнали змін, дозволяють говорити про створення базису для розробки на його основі пасивного універсального методу виявлення порушення цілісності ЦЗ, ефективність якого буде забезпечуватися, зокрема, в умовах незначної збурної дії, над чим зараз працюють автори.

Список використаних джерел:

1. Василенко В. С., Воробей А. П. Цілісність інформаційних об’єктів та код умовних лишів. URL: http://conferences.neasmo.org.ua/ru/art/2364 (дата звернення: 06.10.2022).

2. Пирцхалава Л. Г., Хорошко В. А., Хохлачева Ю. Е., Шелест М. Е. Информационное противоборство в современных условиях. Киев: ЦП «Компринт», 2019. 226 с.
3. Українська Революція гідності, агресія РФ і міжнародне право / за заг. ред. О. В. Задорожнього. Київ: К.І.С., 2014. 1013 с.
4. Shwetha B., Sathyanarayana S.V. Digital image forgery detection techniques: a survey. *ACCENTS Transactions on Information Security*. 2017. Vol. 2 (5). P. 22-31.
5. Mahdian B., Saic S. A bibliography on blind methods for identifying image forgery. *Signal Processing: Image Communication*. 2010. Vol. 25 (6). P. 389-399.
6. Ansari M. D., Ghrera S. P., Tyagi V. Pixel-based image forgery detection: A Review. *IETE Journal of Education*. 2014. Vol. 55 (1). P. 40-46.
7. Block size forensic analysis in digital images / S. Tjoa et al. *2007 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'07)*. Honolulu, 2007. P. 1-636.
8. 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. Springer, 2008. Vol. 5450. P. 229-239.
9. Nouri R., Mansouri A. Digital image steganalysis based on the reciprocal singular value curve. *Multimedia Tools and Applications*. 2017. Vol. 76. P. 8745-8756.
10. Зоріло В. В., Кіосєва О. І., Зоріло І. В. Модифікація алгоритму виявлення штучного підвищення різкості цифрового зображення. *Інформатика та математичні методи в моделюванні*. 2018. Вип. 8 (2). С. 156-163.
11. Li H., Luo W., Qiu X., Huang J. Image forgery localization via integrating tampering possibility maps. *IEEE Transactions on Information Forensics and Security*. 2017. Vol. 12(5). P. 1240-1252.
12. Лебедева Е. Ю. Метод локализации и идентификации оригинальной и клонированной областей изображения. *Інформатика та математичні методи в моделюванні*. 2014. Вип. 4 (1). С. 76-84.
13. Лебедева Е. Ю., Кобозева А. А. Основы метода выявления клонированных участков изображения, подвергнутых коррекции яркости. *Сучасна спеціальна техніка*. 2013. Вип. 3 (34). С. 17-24.
14. Трифонова К. О. Метод виявлення порушення цілісності цифрового зображення шумом Перліна. *Радіоелектроніка, інформатика, управління*. 2017. Вип. 2. С. 134-142.
15. Kowalski, J.P., Peksinski, J., Mikolajczak, G. detection of noise in digital images by using the averaging filter name COV. *Intelligent Information and Database Systems (ACIIDS 2013)*, Lecture Notes in Computer Science, vol. 7803. Springer, 2013. P. 1–8
16. Швідченко І. В. Аналіз програмного забезпечення зі стеганоаналізу. *Штучний інтелект*. 2012. Вип. 3. С. 487-495.
17. Chaeikar S. S., Zamani M., Azizah Bt Abdul Manaf, Zeki, A.M. PSW statistical LSB image steganalysis. *Multimedia Tools and Applications*. 2018. Vol. 77. P. 805–835.
18. Chaeikar S. S., Ahmadi A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. *Signal Processing: Image Communication*. 2019. Vol. 70. P. 233-245.

19. 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. Vol. 17 (2). P. 128-137.
20. Бобок І. І. Дослідження змін властивостей параметрів блоків цифрового зображення при блоковій обробці як основа методу виявлення порушення його цілісності. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2018. Вип. 2 (36). С. 56-67.
21. Кобозева А. А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. *Праці Одеського політехнічного університету*. 2014. Вип. 2. С. 136-146.
22. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности: монография. Киев: ГУИКТ, 2009. 251 с.
23. 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. Vol. 1. P. 140-161.
24. Гонсалес Р., Вудс Р. Цифровая обработка изображений. Москва: Техносфера, 2006. 1070 с.
25. Bergman C., Davidson J. Unitary embedding for data hiding with the SVD. *Security, steganography and watermarking of multimedia contents VII, SPIE*. 2005. Vol. 5681. P. 619–630.
26. Деммель Д. Вычислительная линейная алгебра: теория и приложения. Москва: Мир, 2001. 430 с.
27. 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.
28. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. *2006 IEEE International Conference on Multimedia and Expo*, Toronto, 2006. P. 549-552.
29. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография: теория и практика. Киев: МК-Пресс, 2006. 288 с.
30. Schisterman E. F., Perkins N. J., Liu A., Bondell H. Optimal cut-point and its corresponding Youden index to discriminate individuals using pooled blood samples. *Epidemiology.* 2005. Vol. 16 (1). P. 73-81.

INVESTIGATION OF THE PROPERTIES OF THE COEFFICIENTS OF THE DISCRETE COSINE TRANSFORMATION AS THE BASIS OF THE METHOD OF DETECTION OF DIGITAL IMAGE INTEGRITY VIOLATION

One of the most common representations of information today are digital images, unauthorized changes of which can lead to negative consequences for an individual, institution, firm, and the state as a whole, which makes the detection of digital image integrity violation one of the most urgent tasks of information security. The main drawback of the existing expert methods is their focus on detecting the results of a specific disruptive action, but in practice the expert often does not have information about the

specifics of an attack on a digital image, while his set of tools is always limited, which can lead to a situation where the investigated digital image is erroneously recognized as original. The first «defense line» here should be methods that are effective regardless of the type of disruptive action, i.e. universal. At present, there are a very small number of such methods in open sources; most of them are not free from shortcomings, the main of which is a significant decrease in efficiency in conditions of minor disturbances. The aim of the paper is to develop a theoretical basis for an effective universal method of detection of digital image integrity violation, in particular, in conditions of minor disturbances. In the course of achieving the aim of the paper: the justified expediency of using a block approach when organizing an examination of the integrity of a digital image; the area of discrete cosine transformation (DCP) of the block is chosen as the area of examination; justified selection of specific DCP coefficients for organizing the detection of violations of the integrity of digital images, the values of which do not depend on the value of the quality coefficient used when obtaining the original image, as well as on the specific type of digital images; the difference in the nature of changes in the selected formal parameters during re-saving of lossy digital images, depending on whether it is original or non-original, is investigated. The obtained results of theoretical studies, which are confirmed by the results of computational experiments, constitute the theoretical basis for the development of an effective universal method of examination of the integrity of digital images, in particular, in conditions of minor disturbances.

Keywords: *digital image, integrity violation, discrete cosine transform, block processing, lossy.*

Отримано: 12.10.2022