

Гончаров Микита Олександрович

аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій
Харківський національний університет імені В. Н. Каразіна, Харків, Україна
ORCID: 0000-0002-9790-7260
E-mail: m.honcharov@student.karazin.ua

Малахов Сергій Віталійович

кандидат технічних наук, старший науковий співробітник, доцент кафедри КІСМіТ
Харківський національний університет імені В. Н. Каразіна, Харків, Україна
ORCID: 0000-0001-8826-1616
E-mail: malakhov@karazin.ua

АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ТА ЗАХИСНИХ ВЛАСТИВОСТЕЙ ПІДГОТОВЧИХ ПРОЦЕДУР ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ

У роботі досліджено обчислювальну складність та захисні властивості початкових етапів гібридного стеганографічного алгоритму, що охоплюють процедури попередньої обробки вихідного контенту, формування масиву серій опорних блоків (ОБ), застосування різних схем розгортки та просторової орієнтації ОБ. Проведено аналіз трьох варіантів згладжування малоінформативних ділянок вихідних зображень та виконано їх оцінювання за часовими характеристиками й піковим співвідношенням сигнал-шум (PSNR). Встановлено, що перший і другий варіанти згладжування забезпечують оптимальний баланс між якістю обробки та обчислювальними витратами, тоді як третій варіант характеризується вищою якістю отримуваних зображень, але є більш ресурсомістким. Досліджено особливості формування, класифікації та кодування масиву серій ОБ, а також оцінено вплив різних схем розгортки на часові витрати й стійкість системи до несанкціонованої екстракції стеганографічного контенту. Визначено, що прості схеми розгортки мають мінімальні часові витрати, але нижчий рівень захищеності, тоді як лінійні, нелінійні, багатопрхідні (кратні) та комбіновані схеми, забезпечують вищий рівень захищеності при помірному зростанні часових витрат. Встановлено, що застосування змін просторового позиціонування ОБ контенту, характеризується помірним зростанням обчислювальної складності алгоритму, але суттєво підвищує стійкість системи до атак, навіть у разі компрометації основних механізмів захисту. Моделювання проводилося на тестових зразках напівтонових (8 біт) зображень, генерованих штучним інтелектом (ШІ). Для цього обрані зображення типу «Портрет» і «Пейзаж» та, додатково, використані скрінсейвери сцен комп'ютерних ігор (шутери). Всі тестові зразки характеризуються різною текстурною насиченістю й локальними перепадами яскравості. Отримані результати підтвердили можливість інтеграції досліджених процедур в межах єдиної багаторівневої системи захисту цифрового контенту. Результати моделювань виявили високу адаптивність застосованих процедур обробки, що підтверджує можливість їх застосування в умовах впливу спорадичних ресурсних обмежень та системах обробки даних реального часу.

Ключові слова: інформаційна безпека, стеганографія, цифрові зображення, несанкціонований доступ, обчислювальна складність, просторова орієнтація, ресурсний консенсус, кодування довжин серій, ДКП.

Вступ

Сучасний розвиток інформаційно-комунікаційних систем (ІКС) супроводжується стрімким зростанням обсягів цифрових даних і активним впровадженням технологій штучного інтелекту та машинного навчання (AI/ML) в процеси їх обробки, обміну й зберігання. Це підвищує швидкодію і адаптивність ІКС, але водночас загострює питання забезпечення конфіденційності, цілісності та прихованості циркулюючої інформації [1-4].

Цифрова стеганографія залишається надійним інструментом захисту інформації, яка не лише захищає зміст повідомлення, а й приховує сам факт його існування [1-2]. Разом із тим розвиток методів машинного навчання та комп'ютерного зору підвищує ефективність стегоаналізу, що ускладнює приховування даних.

У цих умовах ключовим завданням є досягнення балансу між надійністю, стійкістю до виявлення та обчислювальною ефективністю алгоритмів. Особливо це актуально для мобільних і вбудованих систем з обмеженими апаратними ресурсами [6-7]. Важливою складовою таких підходів є аналіз обчислювальної складності базових процедур, що визначає їх практичну придатність. Для цього застосовують попередню обробку [7-10], різні схеми розгортки блоків [11-14], формування масивів опорних блоків (ОБ) і механізми їх просторової

орієнтації [14-17]. Проведене моделювання свідчить, що такі підходи базуються на простих оборотних трансформаціях і не потребують значних обчислювальних ресурсів, водночас підвищуючи ефективність приховування цільового контенту [1-4].

Незважаючи на відносну простоту реалізації, ці операції не погіршують візуальну якість контейнера [5], але істотно ускладнюють несанкціоновану екстракцію даних [11-19]. Це підтверджує доцільність використання таких методів і зумовлює необхідність подальшого аналізу їх характеристик для покращення ефективності відповідних алгоритмів в умовах спорадичного впливу ресурсно-часових обмежень [6-7, 17].

Постановка проблеми

Перспективним напрямом розв'язання зазначених вище труднощів є розроблення гібридних стеганографічних методів, здатних забезпечувати багаторівневий захист даних за мінімальних витрат залучених ресурсів [6]. Їх використання дозволяє реалізувати парадигму контрольованої інкапсуляції корисного контенту, параметри якої визначаються структурою ключа екстрактора даних [17].

Порушення або некоректне відтворення його параметрів (*тобто атака*), унеможлиблює відновлення прихованого контенту. Водночас, досягнення такого ефекту не повинно суперечити вимогам до ресурсної ефективності спеціалізованого алгоритму, що зумовлює необхідність аналізу обчислювальної складності відповідних процедур обробки та оцінювання доцільності їх застосування в умовах існування ресурсно-часових обмежень.

Аналіз останніх досліджень і публікацій

Основою для подальшої оцінки ресурсної ефективності досліджуваного стеганоалгоритму, є результати низки попередніх досліджень [7-19]. В них проаналізовано обчислювальну складність процедур передобробки вихідних даних, властивості різних схем розгортки, особливості зміни просторової орієнтації ОБ контенту, та визначено частку їх впливу на загальну ресурсоємність процесу. Відповідно до обраної концепції стеганографічного алгоритму [7], проведено моделювання різних варіантів передобробки, які забезпечують згладжування малоінформативних ділянок зображень [7-10].

За результатами випробувань отримано оцінки продуктивності за часом виконання, показником PSNR (пік сигнал/шум) та кількістю сформованих ОБ для різних типів зображень. Підкреслено, що процес формування масиву серій ОБ, є базовою умовою для подальшого покращення енергоефективності спеціальних перетворень [11-14].

Аналіз властивостей різноманітних схем сканування (розгортки) ОБ, дозволив встановити коректні діапазони налаштувань алгоритму для різного типу контенту [11-12]. Отримані результати дають змогу уточнити специфіку формування масивів серій ОБ для напівтонових зображень, враховуючи особливості обраної схеми розгортки. Вибір схеми розгортки є критичним, оскільки впливає, на можливості прискорення обчислень, що є принциповим для систем реального часу.

Крім того, діюча схема розгортки визначає структуру викривлень, які проявляються на зображенні внаслідок спроб несанкціонованого вилучення контенту (далі атак). В роботах [13-19] досліджено можливості зміни просторової орієнтації наявних ОБ контенту, як додаткового механізму протидії спробам неавторизованого вилучення контенту.

Мета та завдання роботи

Метою даної роботи є оцінка обчислювальної складності 2-х перших етапів дослідного стеганоалгоритму та визначення впливу різних схем розгортки та/чи змін просторової орієнтації ОБ контенту, на стійкість до спроб його неавторизованого вилучення в умовах реалізації різних сценаріїв атак.

Для вирішення поставленої мети, в межах роботи вирішувалися наступні завдання:

- проведено імітаційне моделювання початкових етапів дослідного алгоритму та уточнено параметри обчислювальної складності досліджуваних процедур при зміні умов обробки та типів вихідних даних;

- досліджено характер впливу та комбінаторика використання різних схем розгортки й просторової орієнтації опорних блоків, на стійкість контенту до спроб його неавторизованої екстракції при реалізації різних сценаріїв атак.

Парадигма реалізованого імітаційного моделювання була сфокусована на дослідженні особливостей процедур, які формують первинний «захисний шар» приховуваного контенту, безпосередньо перед реалізацією основних Етапів мультиплексування елементів масиву довжин серій [11-14]. Отримані результати дають змогу уточнити особливості формування масивів серій ОБ напівтонових зображень та оцінити обчислювальну складність відповідних процедур. Проведене моделювання демонструє наслідки умовних атак і підтверджує припущення, що поєднання запропонованих механізмів обробки, покращує адаптивність та підвищує стійкість стеганографічного алгоритму до спроб несанкціонованого вилучення даних з контейнеру - переносника.

Основна частина

Спрощена схема тестового алгоритму та призначення функціональних модулів

Проведене імітаційне моделювання включало наступні процедурні блоки:

- різні варіанти передобробки (згладжування) вихідних зображень [7-10];
- формування серій ОБ з додатковим критерієм структурної автентичності [18-19];
- використання різних схем розгортки [11-14];
- застосування просторових перетворень ОБ контенту [14-16];
- використання зворотних операцій для реконструкції підсумкового зображення після виконання відповідних операцій.

Зазначена комбінація дій дозволяє оцінити вплив перших двох етапів алгоритму на стійкість стеганографічної системи й обчислювальну складність алгоритму [7]. У процесі моделювання варіювалися ключові параметри:

- порогові значення різниці яскравості елементів зображень P_{Z1} та P_{Z2} (що відповідають різним етапам алгоритму обробки);
- розмірність ОБ «N»;
- схеми розгортки ОБ контенту;
- схеми просторових маніпуляцій ОБ контенту.

Такий підхід дозволяє визначити вплив окремих параметрів на структуру масиву серій ОБ, оцінити обчислювальну складність етапів та внесок окремих складових у загальну стійкість контенту. Оцінювання проводилося за критеріями часу виконання процедур та значення метрики PSNR [1-2]. Комплексне варіювання зазначених вище параметрів, дозволяє суттєво ускладнити задачу неавторизованої екстракції даних, навіть у разі компрометації основних механізмів мультиплексування елементів отримуваних масивів серій ОБ [14].

В межах моделювання досліджено 3 варіанти передобробки малоінформативних областей, де умовно «нульовий» варіант (без передобробки) не змінює вихідну структуру даних і використовується лише для порівняння з іншими. Перший і другий варіанти мають однакову обчислювальну складність і є доцільними для умов обмежених ресурсів. Третій варіант забезпечує порівняно найвищу якість згладжування, проте є ресурсномістким і малоприслужним для оперативної обробки великих зображень [7-10].

Діюча схема розгортки визначає порядок обходу (сканування) попередньо згладженого масиву вихідних даних у відповідності з основною парадигмою методу кодування довжин серій [11-14, 18]. Це дозволяє отримати відповідний масив серій ОБ, де для кожного з них, потім, проводиться дискретне косинусне перетворення (ДКП). Схеми розгортки поділяються на лінійні, нелінійні, багатопрохідні (кратні) та комбіновані (рис. 1, [11-12]). Як свідчить моделювання, використання різних схем розгортки є ефективним і обчислювально простим засобом підвищення захищеності даних. У ресурсно-обмежених умовах, зокрема при застосуванні зигзагоподібних або кратних схем [11, 13, 15], вони можуть використовуватися, як самостійний й обчислювально простий інструмент з протидії неавторизованому доступу до

контенту. Проведене моделювання підтверджує, що зигзагоподібні та кратні схеми забезпечують найбільше ускладнення спроб несанкціонованого вилучення вихідного контенту [11-13]. Отримані результати підтверджують ефективність використовуваного підходу, оскільки він враховує умови перевірки структурної подібності сусідніх (за схемою розгортки) блоків зображень. Аналіз виконувався за критерієм різниці між *max* та *min* значеннями яскравості елементів сусідніх блоків: якщо вона перевищувала поріг P_{Z2} , то блок класифікувався, як відмінний від попереднього, та маркувався як новий ОБ. В іншому випадку, блок вважався подібним до попереднього ОБ і таким чином доповнював попередню серію, ще одним елементом [18-19]. Результати моделювання показали, що зі збільшенням розмірності блоків від 4×4 до 16×16 ел., час формування масиву довжин серій ОБ, зменшується приблизно з 0,6 с до 0,15 с. Це забезпечує стабільно передбачуване зменшення часових витрат і дозволяє масштабувати алгоритм для зображень високої роздільної здатності, без суттєвої втрати продуктивності на виконання вказаних процедур [11-14, 18-19].

Під зміною просторової орієнтації ОБ контенту, розуміється застосування до ОБ серій, відповідних геометричних перетворень [14-17], зміст яких визначається відповідним елементом в структури ключа екстрактора даних. Такі операції є обчислювально простими та оборотними, однак суттєво змінюють порядок зчитування пікселів у разі спроб помилкового відновлення ОБ. У практичному сенсі це означає, що навіть за правильно визначених схеми розгортки та розмірності блоків (N), відновлене зображення зазнає суттєвої фрагментації й втрати цілісності сцени, що унеможливорює візуальну або автоматизовану ідентифікацію об'єктів [14-16]. Таким чином, просторові перетворення наявних ОБ, забезпечують захист контенту не за рахунок збільшення складності обчислень, а завдяки широкій комбінаторики можливих станів відповідного елементу складового ключа екстрактора даних [17]. Причому, обчислювальна складність просторових перетворень ОБ, є низькою і, як правило, лінійною відносно кількості пікселів. Досліджувані етапи алгоритму, розглядаються на прикладі зразків зображень генерованих штучним інтелектом (ШІ). Для цього були використані зображення типу «Портрет», «Пейзаж», а також сцен з комп'ютерної гри. Всі ці зразки характеризуються високою текстурною варіативністю й значними локальними перепадами яскравості, що дозволяє всебічно оцінити ефективність розглянутих процедур у складних умовах обробки. Такий вибір тестових даних забезпечує показовість експериментів та дозволяє моделювати різні сценарії формування цифрового контенту, близькі до реальних умов експлуатації.

На рис. 1 наведено спрощену схему перетворень для формованого масиву серій ОБ, яка наочно ілюструє основну сутність процедур, що виконуються в межах реалізованої концепції комп'ютерного моделювання. Представлена схема дозволяє отримати загальне уявлення про структуру й послідовність дій, підкреслюючи ключові особливості підходу без надмірного заглиблення у специфічні технічні деталі. Надана візуалізація сприяє швидкому розумінню логіки роботи зазначеного процедурного ланцюжку та взаємозв'язків між окремими Етапами всього процесу. У подальшому кожен Етап алгоритму розглядається послідовно з метою деталізації його функціонального призначення та ролі в загальному алгоритмі.

На першому кроці дослідного алгоритму здійснюється зчитування вихідного тестового зображення (крок 1, рис. 1), яке передається на подальші Етапи обробки.

На другому кроці (крок 2, рис.1) виконується процедура згладжування вихідних даних [7-9]. Для цього використовуються один із варіантів згладжування, поріг закруглення (P_{Z1}) та розмірність блоків N . Поріг P_{Z1} визначає різницю яскравості між сусідніми пікселями в межах одного блоку зображення. У результаті процедури згладжування, зменшується помітність і кількість локальних перепадів яскравості [7-10].

На 3-му кроці, відповідно до обраної схеми розгортки, виконується послідовний обхід блоків згладженого зображення за заданою траєкторією.

На 4-му кроці формується масив серій ОБ (сукупність ОБ та параметрів їх довжини). Отриманий масив може оброблятися повністю або бути розділеним на парні й непарні

елементи. Дані зберігаються у вигляді лінійного масиву розмірності $1 \times X$ (залежно від повного або двохпрохідного режиму обробки), де X – загальна кількість ОБ та їхніх довжин у зображенні. Така структура (ОБ + довжина) використовується на наступних етапах алгоритму та формується методом кодування довжин серій [23], що враховує умови перевірки подібності змісту сусідніх блоків (за критерієм P_{22}). Отриманий масив серій використовується для подальшої обробки [16], зокрема для реалізації процедур багаторівневого мультиплексування [14] та формування впорядкованої структури даних для наступних етапів перетворень і аналізу.

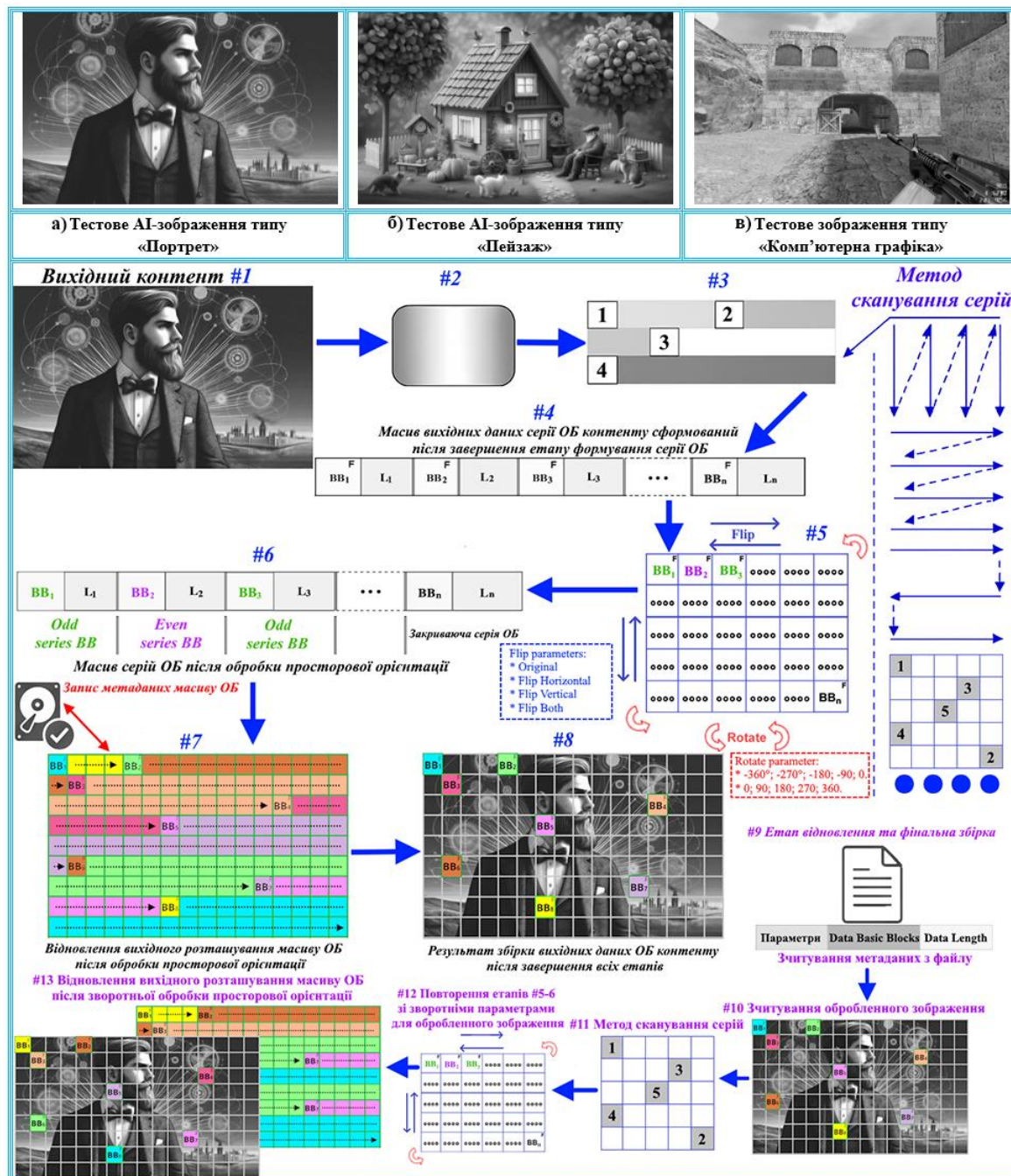


Рис. 1. Спрощена схема перетворень поточного масиву серій ОБ

На 5-му кроці для кожного ОБ, представленого у вигляді лінійного масиву розмірності $1 \times X$, формується двовимірний масив $A \times B$ ($A \times B = X$), де A – висота, B – ширина масиву [16]. Параметри A та B обираються відповідно до заданої користувачем стратегії обробки. Таке

повернення до двовимірної структури посилює наслідки хибного відновлення взаємного розташування блоків і ускладнює підбір правильних параметрів кодування. Якщо X є простим числом, до масиву додається нульовий елемент для уникнення виродженої структури $1 \times X$, оскільки в цьому випадку геометрична обробка не змінює його вигляду та взаємного розташування ОБ. Унаслідок цього відсутні візуальні та статистичні відмінності між правильною і хибною орієнтацією, що нівелює захисний ефект перестановки. Додавання «нульового» елемента дозволяє сформувати масив придатної розмірності для подальших геометричних перетворень. Після обробки «нульовий» елемент вилучається [16]. До сформованого масиву застосовуються наступні геометричні перетворення: – обертання, горизонтальне та вертикальне віддзеркалення, а також їх комбінації. Вибір конкретної операції для кожного ОБ визначається відповідним елементом ключової послідовності, що забезпечує 13-26 варіантів перетворень, що додатково посилює стійкість контенту до спроб його неавторизованого вилучення. Як свідчать експерименти, навіть за компрометації параметрів мультиплексування неправильна орієнтація ОБ призводить до значної просторової фрагментації та втрати цілісності відновлюваного зображення [17].

На 6-му Етапі формується підсумковий масив довжин серій ОБ. Слід зазначити, що значення довжин серій на даному Етапі не підлягають додатковим перетворенням і зберігаються без змін, оскільки їх модифікація виконується вже на наступному Етапі, якій в даній роботі не розглядається. У межах цієї роботи здійснюється відновлення ОБ після обробки, як результуючого зображення, що відображає сукупний ефект від застосованих методів просторової орієнтації наявних ОБ.

На 7-му етапі виконується реконструкція структури даних на основі кодування довжин серій [19], що отримані на 6-му етапі. Перший елемент кожної серії визначається як ОБ з урахуванням виконаної схеми його просторової обробки. Далі здійснюється відновлення ОБ і довжин серій у їх початковому порядку. В результаті формується впорядкована структура, що відображає нове розміщення ОБ у просторі відновленого зображення. На цьому Етапі, додатково, формується та зберігається файл метаданих, у якому фіксуються результати реконструкції масиву ОБ, зокрема: - номери блоків і розмірність двовимірного масиву, сформованого на 5-му Етапі. Цей файл забезпечує можливість «лабораторного» відтворення процесу реконструкції та використовується на наступних Етапах для відновлення ОБ у їх початкових позиціях після їх зсуву чи мультиплексування.

На 8-му Етапі виконується фінальна реконструкція зображення шляхом об'єднання обробленого масиву ОБ і довжин серій у двовимірну структуру. Збірка здійснюється за зворотною схемою розгортки, у результаті чого блоки розташовуються відповідно до заданої структури. При цьому перемішані ОБ залишаються у зміненому порядку, а інші без змін. Отримане зображення є кінцевим результатом роботи алгоритму та відображає сукупний ефект усіх Етапів обробки.

На 9-му Етапі здійснюється зчитування службового файлу метаданих, сформованого на попередніх етапах алгоритму, з метою відновлення вихідного розташування масиву ОБ. Файл містить параметри реконструкції, зокрема розмірність двовимірного масиву (сформованого на 5-му етапі), номери ОБ та службові позначки, необхідні для коректного відновлення просторової структури. Метадані використовуються, як керуючі параметри для подальших операцій і забезпечують узгодженість етапів зворотної обробки.

На 10-му Етапі виконується зчитування результуючого зображення, отриманого після просторових перетворень, яке передається на подальшу обробку.

На 11-му Етапі виконується розбиття зчитаного зображення на блоки відповідно до заданої схеми розгортки, визначеної на кроці №3. Розбиття здійснюється згідно із заданою розмірністю, що забезпечує однозначну відповідність між просторовим розташуванням пікселів і структурою ОБ. У результаті формується множина блоків фіксованого розміру, яка використовується для виконання зворотних операцій. Коректність відновлення зображення

залежить від узгодженості параметрів обробки. Помилка у будь-якому з них, призводить до суттєвих візуальних спотворень.

На 12-му Етапі виконуються зворотні операції відповідно до процедур, застосованих на Етапах №5-6. У межах цього процесу здійснюється декодування масиву серій, відновлення структури ОБ та інверсія перетворень відповідно до збережених параметрів. На цьому Етапі враховуються всі «службові» дані, включно з розміщенням ОБ та параметрами просторових трансформацій, що забезпечує коректне відтворення проміжної структури даних.

На 13-му Етапі виконується відновлення вихідного розташування ОБ після зворотної обробки просторової орієнтації. З урахуванням інформації з метаданих відновлюється початкова послідовність блоків та їх просторове розміщення. У результаті формується структура даних, що відповідає стану до застосування геометричних перетворень.

Запропонована спрощена схема тестового алгоритму [7] та представлені функціональні модулі, забезпечують узгоджену багаторівневу обробку зображень із поетапним переходом: - від просторового представлення до лінійних структур і подальшою реконструкцією вихідних даних. Така організація процесу дозволяє поєднати всі розглянуті операції (згладжування, формування та групування блоків, просторових перетворень і зворотного відновлення) в єдиний цикл із контрольованими параметрами обробки на кожному Етапі. Результати імітаційного моделювання підтверджують коректність функціонування запропонованої схеми обробки (рис.1), її адаптивність до різних типів вхідних даних та посилення стійкості контенту до спроб його неавторизованого вилучення.

Обчислювальна складність початкових етапів алгоритму

Коротко розглянемо результати оцінки складності процедур згладжування. Оцінка здійснювалась з урахуванням: - часових характеристик, впливу розмірності блоків і параметрів згладжування на якість зображення (*PSNR*) та обчислювальної ефективності застосованих процедур. Часові характеристики для різних варіантів обробки наведено в табл. 1. У даному прикладі використано матриці згладжування розміром 3×3 та 11×11 ел., що демонструє вплив їх розмірності на обчислювальну складність [7-10].

Таблиця 1

Час виконання операцій для різних варіантів обробки [с]

Тестове зображення	БЕЗ обробки		Вар. №1		Вар. №2		Вар. №3	
	Розмірності блоків (N×N)							
	3×3	11×11	3×3	11×11	3×3	11×11	3×3	11×11
«Портрет» (AI)	0.0102	0.00092	0.425	0.4916	0.4848	0.6286	1.943	7.9804
«Пейзаж» (AI)	0.014	0.00078	0.4304	0.41318	0.5084	0.6638	1.9772	4.636
«Комп'ютерна графіка»	0.0088	0.00018	0.415	0.487	0.4762	0.6298	1.8154	5.0458

Прим: - Середній час виконання 5-ти однократних повних циклів процедур згладжування

На рис. 2, представлені використані в ході моделювання зразки тестових зображень та наведено результати застосування другого варіанту згладжування [7] при різних параметрах налаштування алгоритму. Значення *PSNR* відображають залежність якості зображень від розміру матриці згладжування та параметра P_{Z1} для різних варіантів обробки.

Такий підхід дозволяє здійснити порівняння досліджуваних методів і оцінити наслідки їх застосування [1-2]. Варто відзначити, що зі збільшенням розмірності маски згладжування спостерігається закономірне зростання обчислювальних витрат, що впливає на загальний час виконання алгоритму. Водночас менші маски забезпечують ефективніше пригнічення

«шумів», що позитивно впливає на кількість сформованих ОБ. При використанні великої розмірності масок, можуть виникати небажані артефакти, що погіршує візуальне сприйняття результату. Отже, вибір потрібної розмірності маски згладжування, забезпечує компроміс між швидкістю та якістю обробки [7-10].

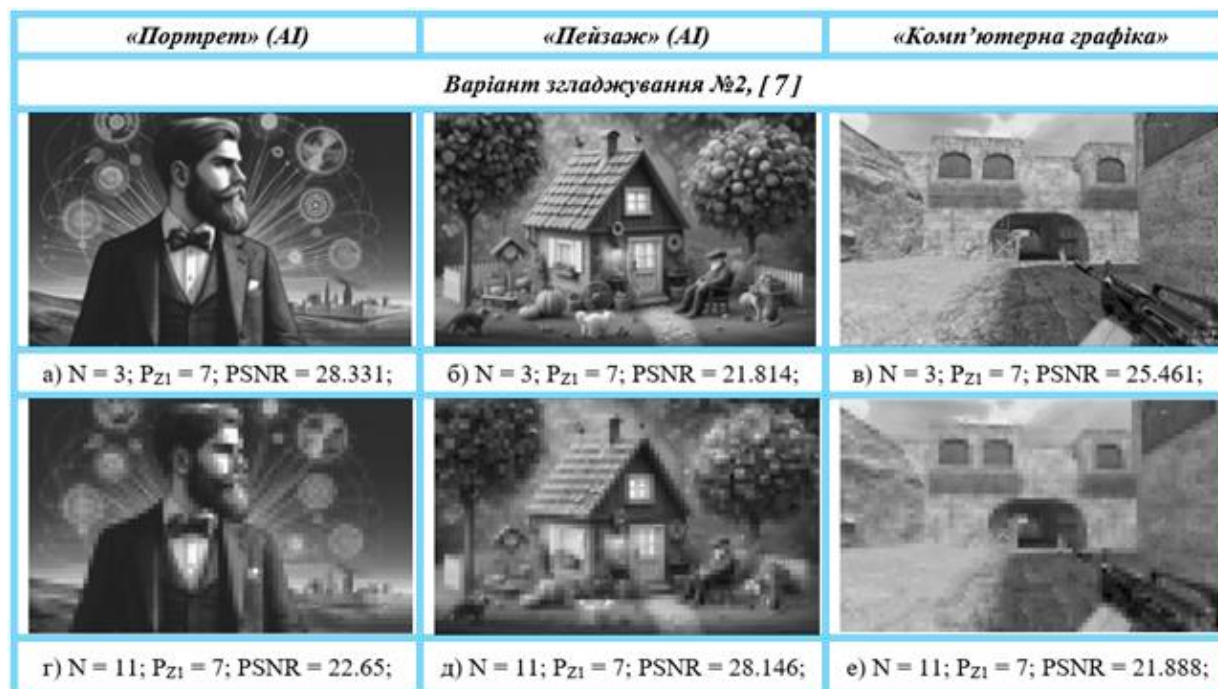


Рис. 2. Порівняння результатів передобробки тестових зображень в умовах варіювання розміру маски згладжування та значення параметра $P_{Z1} = 7$

Збільшення розмірності ОБ та параметра P_{Z1} , зменшують кількість формованих серій ОБ, що звужує базу можливих перестановок на Етапі мультиплексування і помітність артефактів [7-10]. Оптимальними параметрами обробки є: - розмірність матриць згладжування від 3 до 5 ел., розмір блоків (N) зображення 6-12 ел., та значення порогу закруглення P_{Z1} у межах 3-14 градацій яскравості. Такий діапазон значень, забезпечує баланс між якістю відтворення зображень (контенту й контейнера), кількістю сформованих ОБ (комбінаторністю наступного мультиплексу) та обчислювальною складністю реалізованих процедур [7].

Результати моделювання підтвердили, що обрані параметри згладжування забезпечують високу адаптивність алгоритму до різного ступеня деталізації зображень [7-10]. Така гнучкість забезпечує перспективи для подальших досліджень і вдосконалення підходів до обробки зображень з урахуванням їх статистичних властивостей [5] та локальних особливостей окремих блоків. Аналіз отриманих результатів також свідчить, що оптимізація початкових Етапів обробки зображень, повинна враховувати не лише обчислювальну складність, але й характерні статистичні особливості вхідних даних [5]. Такий підхід сприяє досягненню бажаного компромісу, між швидкістю та якістю отриманих результатів.

На рис. 3 представлені приклади обробки тестових зображень для різних схем розгортки. Дослідження проводилося на 3-х зразках після їх попередньої обробки (див. рис. 2(а-в)), в умовах налаштувань, які є найбільш збалансованими з точки зору ефекту згладжування текстур [7]. Оцінка обчислювальної складності (табл.1; див. також у роботах [8-10]) та візуалізація реалізованих схем розгортки (див. рис. 1 в роботі [11]), дозволили проаналізувати характер спотворень (рис. 3), що виникають під час атаки з використанням помилкової розгортки «По рядках» (рис. 1(б) в [12]). Рівень спотворень на отриманих зразках рис. 3 є настільки значним, що візуальна ідентифікація вихідного зображення (рис. 1 (а-в)) стає неможливою без додаткової інформації. Проведене моделювання підтверджує

результативність використання запропонованих підходів, як ефективного інструменту з протидії спробам неавторизованого вилучення стеганографічного контенту та високу гнучкість налаштувань параметрів обробки, що сприяє підтримці потрібного ресурсного консенсусу [6-7].

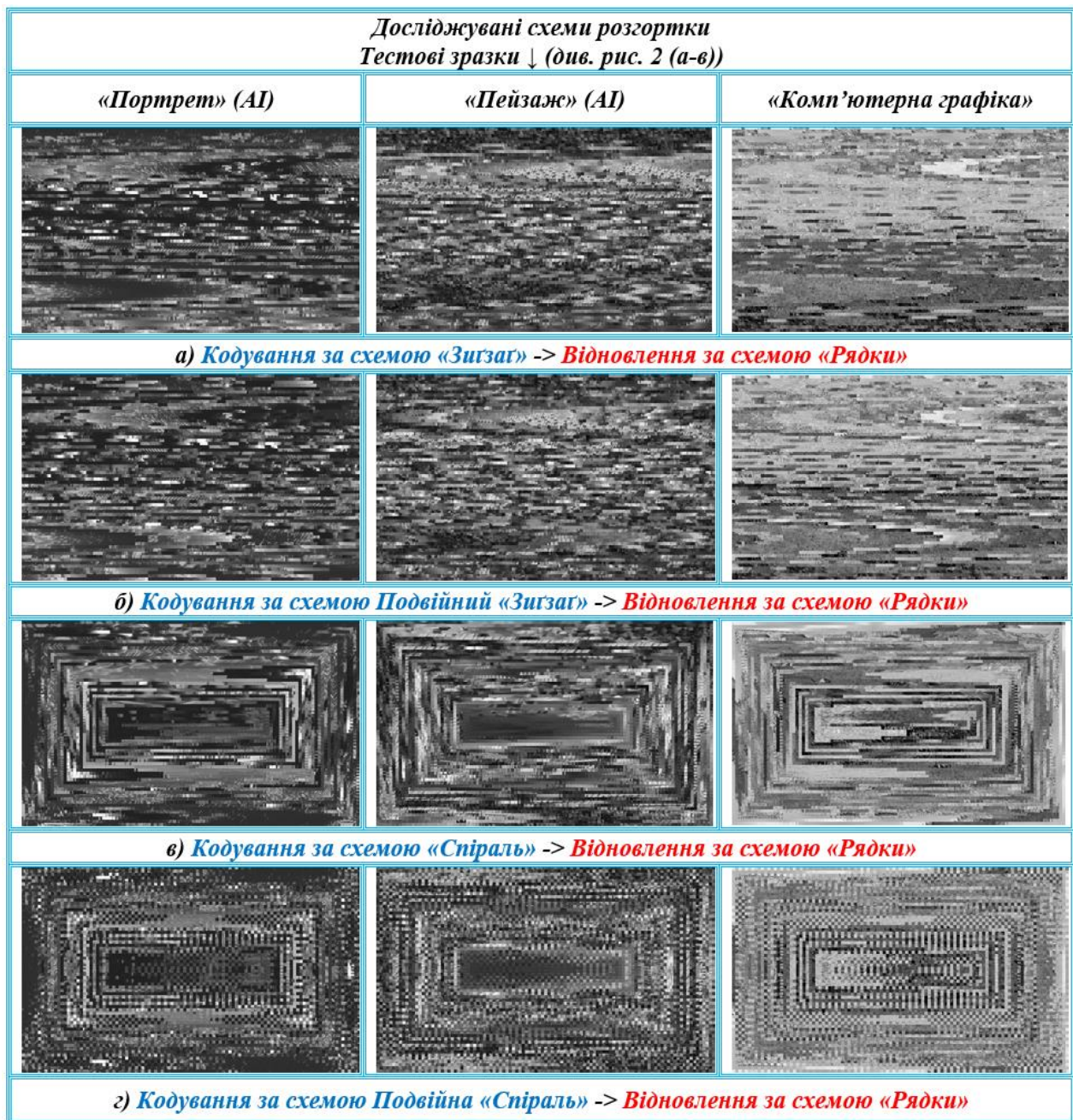


Рис. 3. Результати атаки тестових зображень БЕЗ врахування етапу передобробки для різних розгортки при ОБ $N=8$ та хибному відновленні за схемою «По Рядках»

Гістограми на рис.4 демонструють залежність значень $PSNR$ від різних схем розгортки для обраних (рис.2(а-в)) тестових зразків за умови збігу використаної розмірності ОБ. Звичайно, що більш вищі значення $PSNR$ свідчать про менші розбіжності між оригінальним і відновленим зображеннями [1-2].

Із наведених на рис. 3 зразків слід, що застосування розглянутих схем розгортки повністю руйнують структуру зображення. Це свідчить про високу ефективність контрзаходів при впровадженні відповідних перетворень.

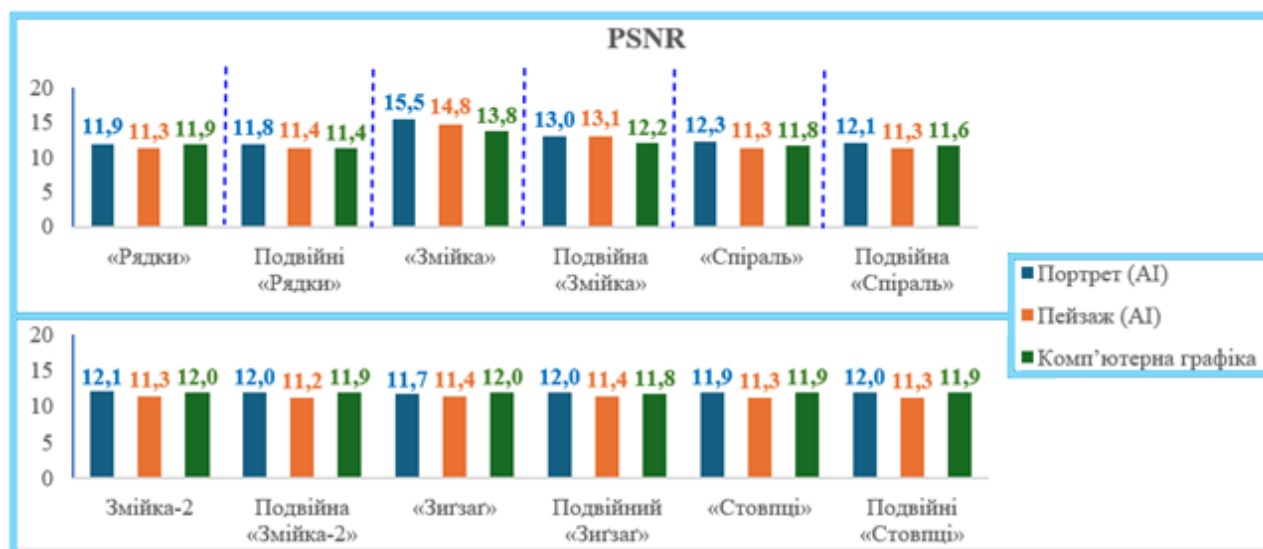


Рис. 4. Значення PSNR для різних схем розгортки БЕЗ врахування етапу передобробки (ОБ 8×8 ел.), для 3-х типів тестових зображень (рис. 1(а-в))

Наведені результати отримані без урахування інших передбачених процедур протидії неавторизованому вилученню контенту, тобто сценарій моделювання був сфокусований на демонстрації наслідків реалізації лише першого рівня захисту [7], пов'язаного з використанням механізму «розгортки». Слід підкреслити, що суміщення принципу кодування довжин серій [19] з механізмом використання різних схем розгортки, одночасно дозволяє вирішити два важливих завдання: 1 – забезпечити ресурсно-необтяжливий рівень захисту; 2 – створити базові умови для зниження обчислювальної складності всього алгоритму на наступних Етапах обробки (особливо на етапі ДКП [5,7]).

Часові характеристики для прямого та зворотного перетворень для різних схем розгортки, наведено на рис. 5. На цих гістограмах представлено середній час виконання процедур формування ОБ зображень розміром 8×8 ел., що дозволяє опосередковано оцінити складність реалізації запропонованих підходів для різних типів контенту.

Час реалізації «простих» схем розгортки [11-12] суттєво менший порівняно з їх більш складними варіантами, що зумовлено меншою кількістю обчислювальних операцій та спрощеною логікою доступу до елементів матриці. Водночас складні схеми зумовлюють більш запутану структуру обробки даних, що істотно ускладнює для атакуючої сторони локалізацію вектора пошуків, щодо діючої комбінації перетворень [11-14]. В цьому сенсі, окрему увагу слід приділити двопрхідним схемам розгортки. Їхня суть полягає у розділенні вихідного масиву на підмножини парних й непарних складових, кожна з яких піддається окремому циклу обробки (за будь якою схемою). В цьому разі при першому проході виконується впорядкування та трансформація значень у межах сформованих груп (парних/непарних).

На другому проході оброблені елементи повертаються у спільну структуру, але вже з новими позиціями та зміненими зв'язками. Такий підхід забезпечує глибоку декомпозицію вихідних даних, що суттєво ускладнює (для атакуючого) оцінку статистичних залежностей між елементами вихідного масиву. Хоча двопрхідні схеми потребують більших часових витрат у порівнянні з однопрхідними реалізаціями, їх використання є виправданим у задачах, де критичною є стійкість до аналізу та атак. Таким чином, вибір між одно- та двопрхідними схемами розгортки серій ОБ, є компромісом між швидкодією та рівнем захищеності. В цілому, більш прості схеми доцільно застосовувати у випадках значних обмежень вільних (доступних) ресурсів, тоді як більш складні варіанти розгортки необхідні, коли безумовним пріоритетом є підвищення складності аналізу та стійкість до несанкціонованого доступу до контенту.

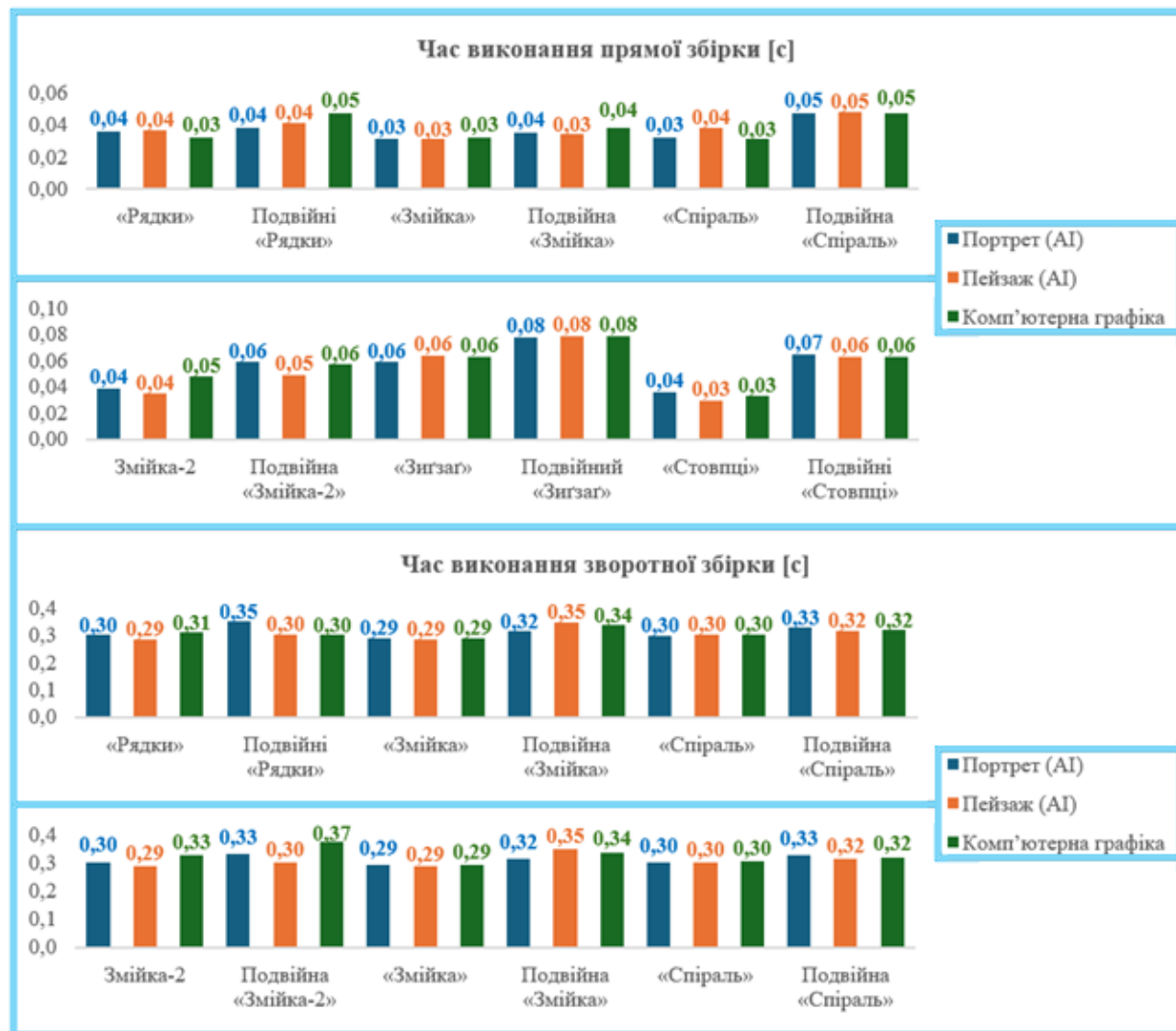


Рис. 5. Обчислювальна складність прямих і зворотних перетворень різних схем розгортки без врахування етапу передобробки для обраних тестових зображень (рис. 1(а-в))

Враховуючи операційну простоту та помірні вимоги до ресурсів, поєднання розглянутих підходів дозволяє сформувати ефективний малоресурсний процедурний ланцюг. Такий підхід зумовлює можливість його практичного використання в умовах впливу спорадичних обмежень на обсяги залучених обчислювальних ресурсів без суттєвої втрати якості й швидкості обробки. При цьому механізми розгортки виступають не лише етапом попередньої обробки, а є ключовим чинником, який визначає обчислювальну складність, часові витрати та загальну ефективність цілої низки подальших перетворень.

За результатами моделювання встановлено, що часові характеристики процесу залежать не лише від використаної схеми, а й від розмірності ОБ, статистичних характеристик вихідних даних та використаних параметрів згладжування, що, в цілому, забезпечує потрібну варіативність обробки. Це, з одного боку, підвищує стійкість стеганографічного перетворення та ускладнює локалізацію параметрів кодування, а з іншого боку – призводить до збільшення навантаження на наступні етапи обробки даних [11]. В цілому, механізм розгортки є важливим елементом реалізованої багаторівневої системи захисту стеганографічного контенту, оскільки його застосування створює потрібні базові умови для скорочення загального часу обробки та реалізації всіх передбачених процедур із захисту контенту. Водночас зростання складності схем супроводжується збільшенням вимог до обчислювальних ресурсів і часу обробки, що визначає необхідність компромісу між: статистичними

властивостями даних контенту й контейнеру, поточними параметрами обробки та бажаним рівнем захищеності даних [11-14]. Наступним кроком досліджень, стало вивчення процедур зміни просторової орієнтації ОБ [13], які виступають одним із додаткових елементів захисту стеганографічного контенту. Впровадження цих процедур дозволяє суттєво ускладнити задачу неавторизованої екстракції даних, навіть за умови компрометації інших передбачених механізмів захисту [14,17]. Тобто, при певних обставинах (злам інших рівнів чи забезпечення питань ресурсного консенсусу тощо), просторові перетворення можуть використовуватись як незалежний рівень захисту або, як складова комбінованої багатошарової системи захисту, що ускладнює аналіз структури даних заповненого контейнера-переносника для стороннього спостерігача. Оскільки обертання чи віддзеркалення не змінюють вихідних статистичних властивостей наявних ОБ, вони не погіршують якість зображення для легітимного користувача, однак створюють суттєві перешкоди для спроб несанкціонованого вилучення контенту. Результати експериментальної оцінки обчислювальної складності процедур зміни просторового позиціонування ОБ, наведено на прикладі обраних тестових зразків (рис. 2(а-в)). В межах моделювання використовувалися тестові зображення, які були обрані й у низки попередніх експериментів [13-16] із застосуванням оптимального варіанту їх передобробки [8-10]. У процесі моделювання аналізувалися часові характеристики виконання різних просторових операцій, та якість відновлення попередньо згладжених зображень, за показником PSNR.

Гістограми рис. 6 характеризують впливу різних схем просторової орієнтації ОБ на якість відновлених тестових зразків, а також на час виконання відповідних просторових операцій. Наведені на рис.6 гістограми, відображають значення PSNR за результатами змін просторової орієнтації ОБ розміром 8×8 ел., для випадків одно- та двохпрохідної (Two-pass) схем розгортки, а також результати оцінки обчислювальної складності процедур зміни просторової орієнтації ОБ (без урахування інших етапів обробки). Перша діаграма ілюструє результати для однопрохідної схеми, а друга для двохпрохідної (Two-pass) схеми. Результати моделювання (рис. 6-7) підтверджують, що введення до структури ключа екстрактора [21] нового елементу, що регламентує зміну просторової орієнтації ОБ, майже не впливає на обчислювальні витрати. Однак, цей елемент суттєво підвищує стійкість системи до несанкціонованого вилучення контенту. Встановлено, що навіть одинична помилка у визначенні параметра орієнтації під час спроб нелегітимної екстракції контенту, призводить до появи значних артефактів, що унеможливають коректне відновлення або навіть класифікацію вихідних зображень.

Слід зазначити, що в лабораторних умовах середній час, необхідний для зворотного відновлення вихідного просторового положення ОБ тестових зображень, знаходиться в межах 4-17,4 с. Відповідно, перебір можливих комбінацій з боку атакуючого, який не володіє параметрами обробки, потребуватиме значно більших часових витрат. Більш того, з урахуванням діапазону можливих налаштувань просторової орієнтації ОБ, а також фактора взаємної комбінаторики всіх елементів ключа екстрактора, процес підбору поточних параметрів обробки контенту є вкрай ресурсоємним завданням. Будь-яка спроба відновлення ОБ без урахування їх просторової орієнтації призводить до порушення відповідності координат блоків пікселів, унаслідок чого формується ефект псевдовипадкового перемішування просторових елементів. Це суттєво ускладнює як візуальний аналіз, так і застосування автоматизованих методів обробки для реконструкції вихідного контенту. Зазначений ефект значно посилюється при використанні двохпрохідних схем та роботі з великою кількістю ОБ, де кількість можливих комбінацій просторових перетворень зростає експоненційно. Отже, можна зробити висновок, що їх поєднання формує багаторівневу систему захисту, котра ускладнює як структурний аналіз контейнера-переносника, так і відновлення прихованого контенту. Такий підхід забезпечує підвищення загальної стійкості контенту до широкого спектра атак, включаючи статистичні, аналітичні та атаки часткового відновлення даних.

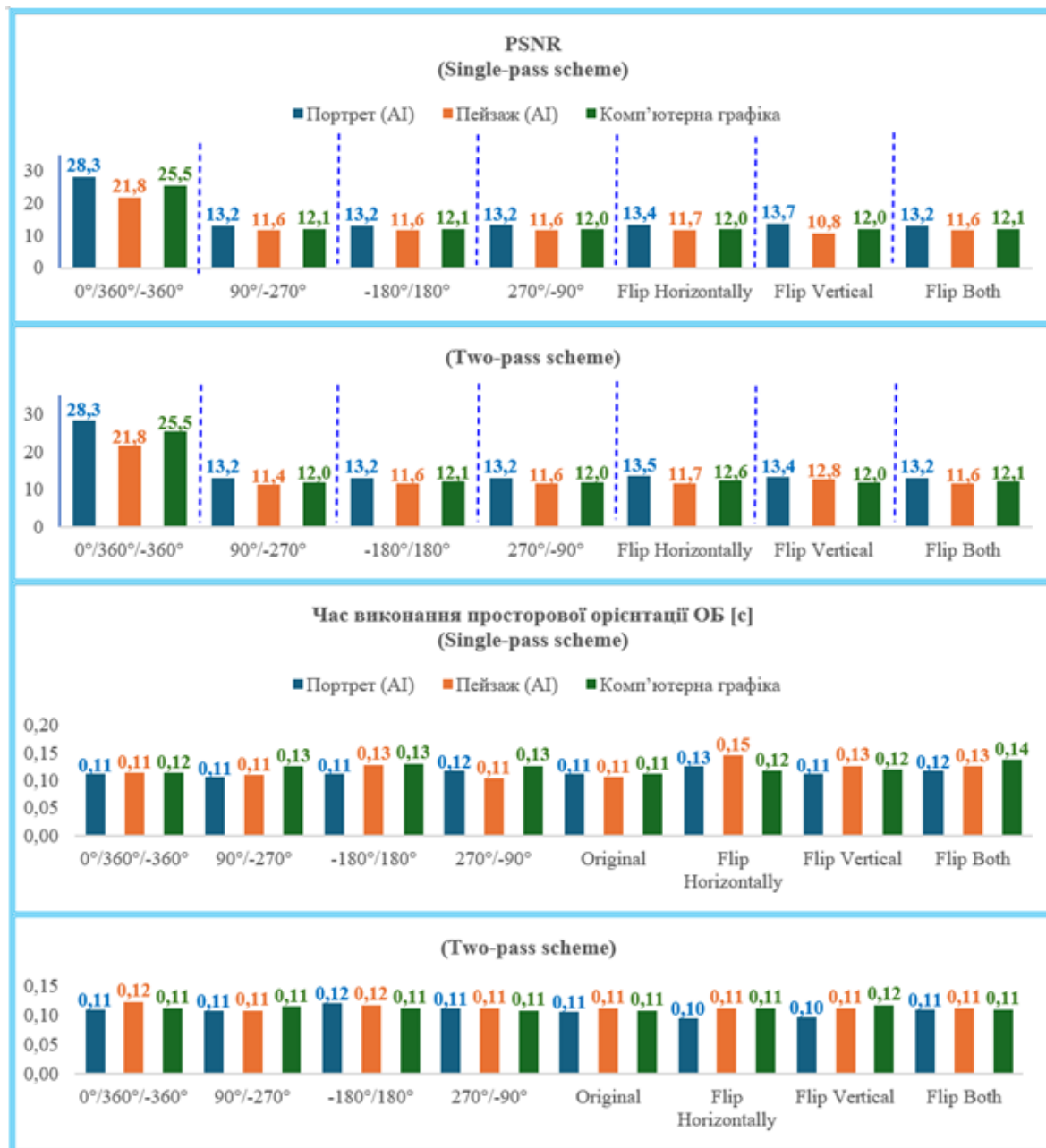


Рис. 6. Значення PSNR за результатами зміни просторової орієнтації ОБ та обчислювальна складність процедур без урахування складності реалізації інших Етапів алгоритму.

На рис. 7, наведено результати спроб несанкціонованого вилучення тестових зображень за умови їх обробки із застосуванням розгортки «По рядках» (рис.1(a) в [11]). У ході моделювання було використано наступні параметри обробки: – маска згладжування 3×3 ел.; – другий варіант згладжування [7]; – поріг закруглення значень яскравості елементів зображень на різних Етапах їх обробки (P_{Z1} та P_{Z2}), рівний 7 градаціям; – розмір блоків 8×8 елементів; – схема розгортки «По рядках»; – двопрхідна схема просторової орієнтації ОБ з різною обробкою на кожному скані (для непарних елементів поворот праворуч на 90° та горизонтальне віддзеркалення, а для парних поворот на -180° й вертикальне віддзеркалення).

У другому стовпці рис. 7 наведені вихідні зображення після обробки 2-м варіантом згладжування, застосування розгортки «По рядках» та зміни просторового позиціонування ОБ за двопрхідною схемою. Отримані зразки є вхідними даними для подальшої імітації спроб несанкціонованого відновлення (вилучення) цих зразків.



Умова атаки: - *вірний підбір розмірності та схеми розгортки ОБ.*
 - *частково відновлена схема просторової орієнтації ОБ.*

Рис. 7. Результати атаки контенту для різних комбінацій підбору діючих параметрів обробки

Важливо, що зворотне відновлення розгортки теж здійснювалось за схемою «По рядках». Тобто, моделювання виконувалося в припущенні, що зломисник правильно визначив використану схему розгортки, що й дозволяє об'єктивно оцінити ефект від застосування просторової орієнтації ОБ. Саме на основі цих зразків у третьому стовпці наведено результати атаки, які відповідають ситуації, коли зломисник «вдало» визначив розмірність ОБ та встановив діючий тип розгортки, проте використав хибну схему просторових перетворень ОБ: замість вертикального віддзеркалення було застосовано горизонтальне, що й призвело до часткового спотворення відновлюваних даних (особливо їх дрібних деталей). Таким чином, послідовність стовпців формує логічний ланцюг операцій: вихідний тестовий зразок → результат попередньої обробки → результат атаки.

Як слід із рис. 7, помилка в діючих параметрах просторових перетворень ОБ, призводить до значної руйнації початкової структури контенту (правий стовпець), навіть за умови «правильного» підбору інших елементів ключа екстрактору даних [17]. Отримані результати підтверджують доцільність інтеграції Етапу просторових перетворень ОБ до структури гібридного алгоритму, що повністю узгоджується з концепцією малоресурсної стегановставки. Використання різних схем просторової обробки ОБ, забезпечує мінімальне зростання обчислювальних витрат та є ефективним засобом підвищення стійкості стеганографічного контенту до спроб його нелегітимної екстракції. Розглянутий підхід забезпечує підтримку необхідного ресурсного балансу в умовах спорадичних обмежень, з боку використовуваних програмно-апаратних платформ та створює передумови для

подальшого розвитку малоресурсних стеганографічних методів та синтезу багаторівневих механізмів захисту.

Висновки

За результатами моделювання початкових етапів дослідного алгоритму уточнено динаміку, характер та типові значення обчислювальної складності досліджуваних процедур. Встановлено, що зміна умов обробки, а саме параметрів згладжування, розмірності ОБ і типу схеми розгортки, впливає на часові характеристики виконання алгоритму, кількість сформованих серій ОБ та рівень візуальних спотворень контенту. Визначено, що 1-й та 2-й варіанти передобробки забезпечують найбільш збалансоване співвідношення між якістю згладжування та обчислювальними витратами, тоді як третій варіант характеризується підвищеною ресурсомісткістю. Середній діапазон часу виконання процедур передобробки для різних типів тестових зображень становить 0.4-8 с залежно від параметрів згладжування та розмірності маски обробки. Збільшення розмірності маски згладжування призводить до закономірного зростання обчислювальних витрат, але забезпечує вищу якість згладжування малоінформативних ділянок зображення.

Дослідження характеру впливу та комбінаторики використання різних схем розгортки й просторової орієнтації ОБ підтвердило, що їх комбіноване застосування суттєво підвищує стійкість контенту до спроб його неавторизованої екстракції при реалізації різних сценаріїв атак. Визначено, що зміна типу схем розгортки та параметрів просторової орієнтації ОБ ускладнює процедури аналізу, реконструкції та відновлення структури зображення навіть за умов часткової компрометації інших параметрів обробки. Використання двопрхідних схем розгортки й комбінованих просторових перетворень ОБ забезпечує суттєве підвищення стійкості контенту при помірному збільшенні обчислювальних витрат, а помилки у відновленні параметрів просторової орієнтації призводять до критичних спотворень відновлюваних зображень.

Реалізація двох перших Етапів розглянутого алгоритму (рис. 1), характеризується залежністю обчислювальних витрат від кількості оброблюваних елементів зображення. Етап передобробки залежить від розміру використовуваної маски згладжування та специфіки виконуваних варіантів згладжування [7]. Зі збільшенням розмірності маски згладжування, очікувано зростає кількість обчислень. Водночас для практично доцільних значень маски (3×3 та 5×5 ел.), обчислювальні витрати залишаються помірними, що робить даний етап повністю придатним для використання в умовах обмежених ресурсів [6, 8, 10]. Застосування згладжування не створює навантаження на систему, але суттєво зменшує обчислювальні витрати на наступних етапах. Крім того, за необхідності, варіювання параметрів згладжування, може покращити поточне співвідношення статистичних властивостей контейнера і контенту, що в свою чергу сприяє оптимізації умов інкапсуляції даних на заключних етапах алгоритму. Етап розгортки та формування масиву серій ОБ, реалізується через послідовний обхід елементів попередньо згладженого зображення та виконання простих операцій порівняння і групування. Його обчислювальні витрати є пропорційними обсягу вхідних даних, оскільки кожен елемент обробляється обмежену кількість разів, без складних вкладених процедур. Використання різних схем розгортки, впливає на кількість допоміжних операцій і особливості доступу до пам'яті, але не призводить до суттєвого ускладнення алгоритму. Кратні схеми розгортки (рис.1 (е),(з), [11]) можуть збільшувати загальну кількість операцій приблизно в 1.5-2 рази, однак це зростання залишається контрольованим і не створює критичного навантаження на обчислювальну систему. Їх використання значно покращує стійкість контенту до спроб проведення стеганоаналізу.

Формування масиву довжин серій ОБ виконується на основі цілочисленних обчислень у межах блоків фіксованого розміру та не потребує значних ресурсів. Час виконання визначається розмірністю ОБ: – зі збільшенням їх розміру, загальна кількість оброблюваних блоків зменшується, що підтверджується скороченням часу обробки (з 0.6 с до 0.15 с при переході від 4×4 до 16×16 ел.). Це забезпечує стабільну передбачуваність потрібних часових

витрат і зумовлює «прозору» масштабованість алгоритму. Впровадження механізмів зміни просторової орієнтації ОБ і варіативність схем розгортки не призводять до істотного збільшення обчислювальних витрат. Відповідні операції зводяться переважно до перестановок індексів та зміни порядку доступу до відповідних елементів. Одночасне застосування обох механізмів, забезпечує суттєве підвищення стійкості контенту до спроб його несанкціонованого вилучення за рахунок широкої комбінаторики можливих станів діючих елементів в структурі ключа екстрактора даних, та критичної залежності отриманого результату від їх правильного відтворення.

Отримані результати демонструють, що перші Етапи розглянутого гібридного алгоритму, створюють ефективний базовий рівень захисту, котрий при широкому арсеналі протидії спробам неавторизованого вилучення контенту та/чи проведення стеганоаналізу, має дуже помірну обчислювальну складність. Досягнутий баланс між ресурсними витратами та ефективністю захисту даних, підтверджує доцільність використання розглянутого підходу в малоресурсних обчислювальних системах, де критичними чинниками є: - обчислювальна продуктивність використовуваних програмно-апаратних платформ, необхідність підтримки режиму реального часу та адаптивність режимів обробки до поточних статистичних характеристикам оброблюваної інформації (в системі ситуативно взаємодіючої пари «контент - контейнер»).

Перелік посилань

1. Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge: Cambridge University Press.
2. Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography* (2nd ed.). Morgan Kaufmann.
3. Кузнецов, О. О., Євсєєв, С. П., & Король, О. Г. (2011). *Стеганографія: навч. посіб.* Вид-во ХНЕУ. <http://www.repository.hneu.edu.ua/jspui/handle/123456789/2289>.
4. Yahya, A. (2019). *Steganography techniques for digital images*. Springer International Publishing.
5. Pratt, W. K. (1978). *Digital image processing*. John Wiley & Sons.
6. Гончаров, М., & Малахов, С. (2024). Аналіз сучасних мобільних платформ для забезпечення процедур стеганографічної вставки. *Grail of Science*, (52), 705–707. <https://doi.org/10.36074/grail-of-science.23.05.2025>.
7. Гончаров, М., Лесная, Ю., & Малахов, С. (2021). Дослідження властивостей прототипу гібридного стеганоалгоритму. *Комп'ютерні науки та кібербезпека*, (2), 45–56. <https://doi.org/10.26565/2519-2310-2021-2-05>.
8. Гончаров, М., Нарєжний, О., & Малахов, С. (2025). Аналіз передумов для забезпечення консенсусу ресурсів при виконанні процедур вставлення стеганографічних даних. *Сучасний захист інформації*, 63(3), 37–47. <https://doi.org/10.31673/2409-7292.2025.030518>.
9. Гончаров, М., Чепель, Д., & Малахов, С. (2025). Оцінка обчислювальної складності етапу попередньої обробки вхідних даних при реалізації процедур стегановставки зображень. *Science and Technology Today*, 8(49), 1228–1245. [https://doi.org/10.52058/2786-6025-2025-8\(49\)-1228-1245](https://doi.org/10.52058/2786-6025-2025-8(49)-1228-1245).
10. Гончаров, М., & Малахов, С. (2025). Моделювання і оцінка обчислювальної складності основних процедур, початкових етапів гібридного стеганоалгоритму. *Комп'ютерні науки та кібербезпека*, (1), 41–59. <https://periodicals.karazin.ua/cscs/article/view/2519-2310-2025-1-04>.
11. Гончаров, М. О., Малахов, С. В., & Жіленков, Д. В. (2025). Дослідження складності та властивостей різних схем розгортки вихідних даних стеганоконтента в умовах зміни сценаріїв атак. *Сучасний захист інформації*, (4), 44–58. <https://journals.dut.edu.ua/index.php/dataprotect/article/view/3352>.
12. Гончаров, М., & Малахов, С. (2023). Дослідження способів розгортки вихідних блоків зображення-стеганоконтенту як механізму протидії від несанкціонованої екстракції даних. *Science and Technology Today*, 4(18), 293–308. [https://doi.org/10.52058/2786-6025-2023-4\(18\)-293-308](https://doi.org/10.52058/2786-6025-2023-4(18)-293-308).
13. Гончаров, М., Малахов, С., & Колованова, Є. (2023). Результати моделювання різних схем просторової орієнтації та розгортки серій опорних блоків зображень для протидії несанкціонованої екстракції стеганографічних даних. *Комп'ютерні науки та кібербезпека*, (2), 58–70. <https://periodicals.karazin.ua/cscs/article/view/23122>.
14. Гончаров, М., & Малахов, С. (2023). Research of procedures for disintegration of the series length array as a mechanism way to confront unauthorized extraction of steganoccontent. *Science and Technology Today*, 6(20), 114–129. [https://doi.org/10.52058/2786-6025-2023-13\(27\)-701-717](https://doi.org/10.52058/2786-6025-2023-13(27)-701-717).
15. Гончаров, М., & Малахов, С. (2023). Моделювання спроб несанкціонованого вилучення стеганоконтенту при зміні параметрів просторової орієнтації опорних блоків контенту. *Science and Technology Today*, 6(20), 114–129. [https://doi.org/10.52058/2786-6025-2023-6\(20\)-114-129](https://doi.org/10.52058/2786-6025-2023-6(20)-114-129).

16. Гончаров, М., & Малахов, С. (2023). Адаптивна модифікація вихідного масиву серій опорних блоків як механізм протидії неавторизованій екстракції стеганокоменту. *Science and Technology Today*, 8(22), 336-352. [https://doi.org/10.52058/2786-6025-2023-8\(22\)-336-352](https://doi.org/10.52058/2786-6025-2023-8(22)-336-352).

17. Honcharov, M., & Malakhov, S. (2024, March 1). Modeling attempts of unauthorized extraction of steganoccontent under different combinations of data key-extractor. *Collection of Scientific Papers «ΛΟΓΟΣ»*, 234-245. <https://doi.org/10.36074/logos-01.03.2024.053>.

18. Малахов, С., & Гончаров, М. (2024). Уточнення процедур формування серій опорних блоків зображень на етапі їх передобробки при реалізації процедур стегановставки. *Grail of Science*, (46), 694-700. <https://archive.journal-grail.science/index.php/2710-3056/issue/view/29.11.2024/34>.

19. Гончаров, М., & Мелкозьорова, О. (2024). Імплементація методу кодування довжин серій для забезпечення процедур стеганографічної вставки зображень. *Комп'ютерні науки та кібербезпека*, (1), 41-48. <https://periodicals.karazin.ua/cscs/article/view/23092>.

Mykyta Honcharov

Postgraduate Student, Department of Cybersecurity of Information Systems, Networks and Technologies

V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

ORCID: 0000-0002-9790-7260

E-mail: m.honcharov@student.karazin.ua

Serhii Malakhov

Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department of KISMiT

V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

ORCID: 0000-0001-8826-1616

E-mail: malakhov@karazin.ua

ANALYSIS OF THE COMPUTATIONAL COMPLEXITY AND SECURITY PROPERTIES OF THE PREPARATION PROCEDURES OF THE HYBRID STECHANOMY ALGORITHM

The paper investigates the computational complexity and security properties of the initial stages of a hybrid steganographic algorithm, which include procedures for preprocessing the source content, forming an array of support block series (SBs), and applying different scanning schemes and spatial orientation of the SBs. An analysis of three options for smoothing low-information areas of the source images was conducted and their evaluation was performed based on time characteristics and peak signal-to-noise ratio (PSNR). It was found that the first and second smoothing options provide an optimal balance between processing quality and computational costs, while the third option is characterized by higher quality of the resulting images, but is more resource-intensive. The features of the formation, classification, and encoding of the SB series array were investigated, and the impact of different scanning schemes on time costs and the system's resistance to unauthorized extraction of steganographic content was also assessed. It was determined that simple scanning schemes have minimal time costs, but a lower level of security, while linear, nonlinear, multi-pass (multiple) and combined schemes provide a higher level of security with a moderate increase in time costs. It was established that the use of changes in the spatial positioning of the content OB is characterized by a moderate increase in the computational complexity of the algorithm, but significantly increases the system's resistance to attacks, even in the case of compromising the main protection mechanisms. The simulation was carried out on test samples of halftone (8 bit) images generated by artificial intelligence (AI). For this purpose, images of the "Portrait" and "Landscape" types were selected and, in addition, screensavers of computer game scenes (shooters) were used. All test samples are characterized by different texture saturation and local brightness differences. The results obtained confirmed the possibility of integrating the studied procedures within a single multi-level digital content protection system. The simulation results revealed high adaptability of the applied processing procedures, which confirms the possibility of their application in conditions of sporadic resource constraints and real-time data processing systems.

Keywords: information security, steganography, digital images, unauthorized access, computational complexity, spatial orientation, resource consensus, series length coding, DCP.

Надійшла до редакції (Received): 04.07.2026

Прийнята до друку (Accepted): 08.09.2026

Опубліковано онлайн (Available online): 15.09.2026

<http://creativecommons.org/licenses/by/4.0/>

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License