Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

Зав.кафедрою БІСТ

Сергій РАССОМАХІН

«02» 12 2022 р.

Пояснювальна записка

до кваліфікаційної роботи
магістра

на тему: «Моделювання та дослідження концепту багаторівневого мультиплексу даних гібридного стеганоалгоритму»

оцінка « » Керівник доцент каф. БІСТ Малахов С.В.

Голова ЕК Рецензент Головний метролог

Доценко С.І. _____ ХНУ імені В. Н. Каразіна

Гостєв О.Л.

Виконавець : студент групи КБ-61

Гончаров М.О.

Харків – 2022

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи магістра містить: 72 сторінки, 37 рисунків, 4 таблиці, 2 додатки, 25 використаних джерел.

Об’єктом дослідження є методи стеганографічного захисту цифрових зображень.

Предметом дослідження є процедури багаторівневої обробки відеоданих.

Основними методами досліджень є комп’ютерне моделювання концепції конструктиву алгоритму, його аналіз та узагальнення отриманих результатів.

Мета роботи є визначення складу і параметрів складеного ключа екстрактора даних стеганографічного алгоритму, та дослідження властивостей основних етапів обробки вихідних даних в межах прийнятої концепції конструктиву алгоритму.

Розроблений дослідний алгоритм забезпечує моделювання основних процедур обробки відеоданих у рамках робот, щодо створення прототипу гібридного алгоритму стеганографічного обробки зображень. Запропонована концепція конструктиву алгоритму дозволяє позиціонувати його, як автономне малоресурсне рішення для забезпечення захисту даних в складі різних мобільних платформ. Досліджені процедури багаторівневого мультиплексу даних забезпечують необхідні механізми з протидії спробам нелегітимної екстракції даних. Визначені основні параметри елементів складеного ключа екстрактора даних для різних типів даних та умов їх обробки, що забезпечує широкий діапазон комбінаторики параметрів кодування. Результати роботи є складовою частиною циклу досліджень, в межах реалізації загального концепту створення прототипу гібридного стеганоалгоритму, та може бути використаний у галузі програмних рішень для мобільних гаджетів та в освітніх цілях для створення дослідних програмних імітаторів основних етапів захисту відеоданих.

Ключові слова: СКП, КЛЮЧ, СТЕГАНОГРАФІЯ, ЗОБРАЖЕННЯ, КОНТЕНТ, АЛГОРИТМ, СЕРІЯ, МУЛЬТИПЛЕКСУВАННЯ, СТЕК, АТАКА, ІНКАПСУЛЯЦІЯ.

ABSTRACT

The explanatory letter to the master's project contains 72 pages, 37 figures, 4 table, 2 appendix, 25 source references.

The object of research is the methods of steganographic protection of digital images.

The subject of research is the procedures of multilevel video data processing.

The main research methods are computer modeling of the concept of the constructive algorithm, its analysis and generalization of the obtained results.

The purpose of the work is to determine the composition and parameters of the composite key of the data extractor of the steganographic algorithm, as well as to study the properties of the main stages of source data processing within the accepted concept of algorithm constructive. The developed research algorithm provides modeling of the main procedures for processing video data as the part of the work on creating a prototype of a hybrid algorithm for steganographic image processing. The proposed concept of the algorithm construct makes it possible to position it as an autonomous low-resource solution for ensuring data protection as part of various mobile platforms. The researched procedures of multi-level data multiplex provide the necessary mechanisms to counteract attempts at illegitimate data extraction. The main parameters of the elements of the composite key of the data extractor for different types of source data and conditions of their processing were determined, which provides a wide range of combinatorics of encoding parameters. The results of the work are an integral part of the cycle of research, within the framework of the implementation of the general concept of creating prototype a hybrid steganoalgorithm, and can be used in the industry of software solutions for mobile gadgets and for educational purposes to create research software simulators of the main stages of video data protection.

Key words: MSE, KEY, STEGANOGRAPHY, IMAGE, CONTENT, ALGORITHM, SERIES, MULTIPLEXING, STACK, ATTACK, ENCAPSULATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ОБ	–	Опорні блоки
ДКП	–	Дискретне косинусне перетворення
ЗДКП	–	Зворотне дискретне косинусне перетворення
СКП	–	Середньоквадратична помилка
PSNR	–	Пікове відношення сигнал-шум

ВСТУП

Добре відомо, що одним із ефективних напрямів забезпечення приховування фактів передачі і зберігання інформації, є застосування різних стеганографічних методів. Цифрова стеганографія, як окремий науковий напрямок, вивчає можливості використання властивостей цифрового контенту різного типу для забезпечення більш ефективного вирішення завдань, що пов’язані с синтезом нових методів і способів прихованої передачі, та маркування цільової інформації (контенту).

Принциповим є те, що в незалежності від використаного напрямку стеганографії, необхідно забезпечувати мінімізацію демаскуючих аномалій використовуваних контейнерів та підтримувати заданий рівень стійкості контенту стосовно спроб його неавторизованої екстракції, а в деяких випадках, і стійкості до спроб навмисного спотворення контейнерів [2,6].

При приховувані (інкапсуляції) в цифрових зображеннях будь-якої іншої інформації (в межах даної роботи - зображень), виникають певні спотворення цих об'єктів – переносників даних (контейнерів). При збалансованих налаштуваннях алгоритму інкапсуляції даних (далі – стеганоалгоритму), можливо забезпечувати рівень спотворень використовуваних зображень-контейнерів, на рівні, що знаходиться нижче порога чутливості зорової системи людини. Це забезпечує фактичну відсутність помітних аномалій переносників інформації та ускладнює роботу атакуючої сторони (включаючи стеганоаналітика). Тим самим забезпечується необхідний баланс між збереженням характерних властивостей для використовуваного типу контейнерів і величиною допустимих спотворень, прийнятних для заданого типу прихованого контенту (далі – стеганоконтенту).

В цьому сенсі зрозуміло, що кількість, структура та інтенсивність проявів різних артефактів зображень контейнеру і контенту, знаходяться в прямий залежності від

коректності обраних для них режимів обробки на всіх етапах діючого стеганоалгоритму [1,2].

При цьому, слід мати на увазі, що при обробці даних контейнерів і контенту можуть бути використані, як однотипні (симетричні) режими обробки, так і режими, які реалізують різні параметри обробки даних (асиметричні) [1,3,5,6]. Такими відмінностями є:

- розмір блоків (фрагментів) зображень на які поділяється вихідний масив;
- параметри попередньої обробки масивів даних контейнерів і контенту;
- критерії оцінки значущої інформації контейнерів і контенту;
- відмінності реалізацій прискорення обчислювальних процедур та інше.

Таким чином, на одних і тих же типах вихідних даних можна отримати дуже різний ефект, з точки зору помітності артефактів та окремих параметрів роботи самого алгоритму стегановставки. Крім того, для авторизованої екстракції контенту потрібна інформація, стосовно діючих параметрів внутрішньо- та міжблокового мультиплексу даних [7,8,9], як для контенту, так і для контейнеру (що відповідає різним рівням обробки). Вся ця інформація, міститься в структурі складеного ключа екстрактора даних [1], де кожен з його елементів визначає поточні режими обробки стеганоконтенту та контейнеру.

Порушення структури ключа екстрактора та/або діючих параметрів (значень) кожного з його окремих елементів, призводить до унеможливлення його вилучення, або суттєвим спотворенням контенту [10,11,12]. Саме дослідженням спостережуваних ефектів та моделюванню зазначених вище питань, на кожному з етапів дослідного алгоритму [1,13,14,15], і присвячена дана робота.

1 АНАЛІЗ МОЖЛИВОСТЕЙ БАГАТОРІВНЕВОЇ ОБРОБКИ ДАНИХ ДЛЯ РІЗНИХ ТИПІВ ЗОБРАЖЕНЬ

Вирішення питань забезпечення оперативної та малоресурсної (малої обчислювальної складності) стегановставки з необхідними показниками скритності факту інкапсуляції даних та стійкості до спроб нелегітимної екстракції прихованого контенту є актуальним завданням.

Створюваний в межах роботи, прототип гібридного алгоритму, використовує різні властивості, ефекти та методи кодування відеоданих [16,19,20].

Обрана концепція створення алгоритму [1] забезпечує широкий діапазон комбінаторики параметрів кодування (для контейнера і контенту), що потенційно розширює варіативність реалізацій, як структури, так і станів кожного з окремих елементів інтегрованого ключа екстрактора даних [1,4,7].

У даному розділі стисло представлені основні результати моделювання процедур формування серій опорних блоків зображень (класифікованих, як блоки з ідентичним змістом), що є одним з важливих етапів створюваного концепту гібридного стеганоалгоритму [4].

Структура дослідного алгоритму містить чотири основні функціональні модулі, що послідовно реалізують усі передбачені етапи обробки даних. Склад основних етапів (для діючого релізу прототипу) має такий вигляд [1,2,4,19-22]:

1) попередня підготовка (аналіз та згладжування) вихідних даних [1,2,17];

2) формування масиву серій подібних (ідентичних за заданими критеріями) блоків зображень [4,20,21];

3) обробка опорних блоків сформованих серій (надалі опорних блоків - ОБ), за допомогою застосування методів кодування з перетворенням (в даному випадку дискретного косинусного перетворення) з подальшою селекцією і квантуванням всіх коефіцієнтів, що зберігаються [6,17,19,20];

4) інкапсуляція контенту, до складу блоків даних зображення-контейнера та багаторівневий мультиплекс (шифрування) отриманих даних [1,6,7,11].

Слід підкреслити, що процедури перших 2-х етапів (згладжування, формування масиву серій ОБ і проведення кодування з перетворенням) можуть в однакової мірі зачіпати масиви даних контейнера і контенту. При збігу цих параметрів обробки, такий режим називається симетричним, а при наявності відмінностей в принципах обробки даних - несиметричним. Відповідний режим обробки даних, формує окрему позицію в структурі інтегрованого ключа екстрактора даних [1,8].

В межах проведених досліджень було реалізовано моделювання тільки симетричного режиму обробки. В цілому, використання спеціальних процедур передобробки даних [4,6] дозволяє забезпечити необхідний диспаритет початкових умов (властивостей об'єктів) для подальшої реалізації стегановставки при зниженні загальної обчислювальної складності всього алгоритму. Вибрана концепція реалізації конструктиву алгоритму дозволяє позиціонувати його як автономне рішення з метою забезпечення захисту даних у складі різних мобільних платформ. При певному доопрацюванні можлива розподілена реалізація алгоритму [1].

Для реалізації процедур першого етапу алгоритму (передобробки вхідних даних) досліджено три варіанти згладжування малоінформативних областей [2,3,20] зображень, з можливістю зміни допустимого значення різниці яскравостей елементів (P_Z) та розміру матриць згладжування на задану величину.

У 1-му варіанті згладжування здійснювалася оцінка різниці значень яскравості центрального елемента з його периферійним оточенням (див. Рис. 1.1). У випадку, якщо отримана різниця менша від заданого P_Z, то елемент у цій позиції заміщався значенням яскравості центрального елемента.

Відповідно до другого варіанту, якщо периферійні значення перевищують яскравість центрального елемента більш ніж величину P_Z, то виконується заміна всіх значень цього блоку на середнє значення яскравості його елементів. В результаті отримуємо покращену версію першого варіанту [2,3,6].

а) б)

Рисунок 1.1 – Варіанти обробки елементів

(*для маски 3×3 (а) та 5×5 елементів (б)*)

Третій варіант забезпечує перебір «всіх з усіма», де головним завданням є пошук елементів, різниця між якими перевищує значення P_Z.

При наявності такої різниці даний блок залишається без змін (оскільки можлива присутність фрагмента контуру), інакше виконується заміна всіх значень цього блоку на середнє значення яскравості його елементів.

За результатами моделювання третього варіанту згладжування встановлено, що при трьох різних типів зображення, з різною ймовірністю перепаду яскравості між сусідніми елементами (табл. 1.1) основні контури зберігаються до $P_z = 14$ (при 256 градаціях яскравості (сірого) для контейнера та контенту) [2,3,19,20].

Імовірністю перепаду яскравості (p) вважається ймовірність випадкової події, яка полягає в зміні значення яскравості між сусідніми елементами зображення уздовж рядка розгортки. Для матриці (блоку) зображення $||A_{ij}||$ розміром $N_i \times N_j$ ймовірність перепаду яскравості визначається по формулі 1.1 [6]:

$$p = \frac{m(\lambda)}{N_i \cdot N_j} \tag{1.1}$$

де p – ймовірність перепаду яскравості,

$m(\lambda)$ – математичне очікування довжини серії,

N_i і N_j – кількість елементів зображення по горизонталі та вертикалі.

Класифікація зображень за імовірністю перепаду яскравості сусідніх елементів наведена в таблиці 1.1 [6].

Таблиця 1.1 – Класифікація зображень за імовірністю перепаду яскравості

Імовірність перепаду яскравості	0.1-0.05	0.05-0.03	0.03-0.01
Тип зображення	Картографічні зображення (*аерофотознімок*)	Портретні зображення	Мнемосхеми

Слід зазначити, що метод довжин серій, який використовується на 1-му етапі дослідного алгоритму, показує хороші результати при обробці зображень, що відносяться до класів мнемосхема і портрет [6].

Проведені дослідження методу довжин серій показали, що він враховує тільки статистичну надмірність [6]. Для забезпечення більш приємних «стартових» умов для початку реалізації процедур 2-го етапу (тобто формування серій ОБ) потрібні відповідні зміни маски згладжування, та порогового значення загрублення (P_Z) кольору/яскравості елементів зображення [6]. Воно характеризує ступінь відмінності між сусідніми елементами зображення, що встановлюється, наприклад, з урахуванням психовізуальних особливостей спостерігача або типу оброблюваного зображення [6].

Також зміна порогу загрублення яскравості (P_Z), дозволяє значно підвищити коефіцієнт стиснення зображення, а його максимальне значення може досягає 25% від використовуваної шкали яскравості (кольору) [6].

Результати обробки зображень різного типу при зміні значень зазначених вище параметрів обробки [1,19], наведені в Додатку Б (див. Рис. Б.4 – Б.12).

Основною метою проведення вище зазначених процедур є створення необхідних стартових умов для формування масивів серій подібних блоків (відповідно для контейнера та контенту) обраної розмірності (2-й етап) з подальшою реалізацією кодування з перетворенням для всіх ОБ отриманих серій [1,2,21].

В рамках реалізації процедур другого етапу передбачена можливість варіювання розмірностями блоків для контенту та контейнера, що створює необхідні умови для компенсації невигідних, з точки зору процесу інкапсуляції даних, вихідних співвідношень (особливості структури зображень) контейнера та контенту [4,13]. При цьому слід враховувати баланс, що складається, між збільшенням розмірністю блоків і зменшенням загального часу обробки, що визначається кількістю сформованих серій ОБ для контейнера і контенту.

У рамках третього етапу моделювання використовується двовимірне дискретне косинусне перетворення (ДКП) [19,20], яке є універсальним за типами оброблюваних даних та має гарну здатність до концентрації найбільш важливої інформації (тобто істотних деталей зображення) у найменшій кількості відліків.

Для фільтрації значущих коефіцієнтів трансформант ОБ [22], використаний доопрацьований зонально-пороговий метод, що забезпечує адаптацію до локальної статистики зображень, що обробляються, при збереженні всіх переваг зонального способу селекції коефіцієнтів перетворення [19].

Облік локальної статистики оброблюваних фрагментів зображень забезпечується за допомогою обчислення середньої амплітуди коефіцієнтів трансформанта (порогового значення селекції), що виключаються, і подальшого збереження деяких з них з найбільшими абсолютними значеннями у визначеній області трансформант.

В рамках четвертого етапу, здійснюється безпосереднє приховування даних контенту масив даних ОБ контейнера. Усі процедури цього етапу мають багаторівневу реалізацію, де кожен із рівнів визначає свою позицію у структурі композитного (складеного) ключа екстрактора даних [1,7].

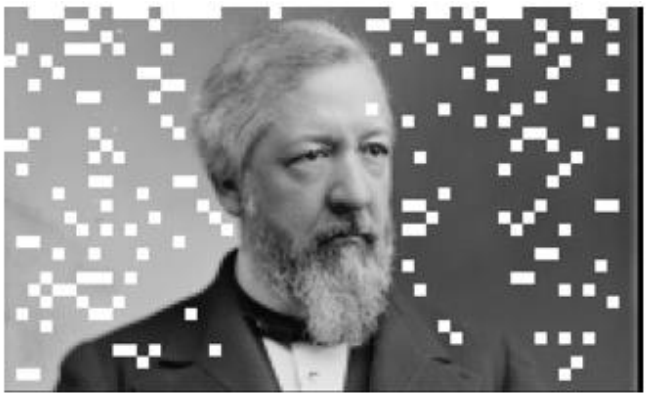
Результати обробки тестового зображення типу «портрет», за допомогою матриці згладжування розміром 5×5 елементів та значенням різниці яскравості елементів $P_Z = 7$ наведені у Додатку Б (див. Рис. Б.1, Б.4, Б.7, Б.10, Б.13 (*а,б*)).

Аналіз масиву помилок (спеціально збільшених по амплітуді для їх локалізації) показує, що практично всі вони сконцентровані в області фону (концентрація «зерна»), але при цьому залишаються нижче порогу візуальної помітності [20].

При цьому області високої детальності зображення (обличчя) фактично не торкнулися, особливо для 2 і 3 варіантів передобробки. Таким чином, мета попередньої обробки досягнута.

На рисунку 1.3. представлені результати «збірки» контейнера для тестового зображення типу «портрет», за результатами виконання трьох етапів тестового алгоритму. На першому рисунку (див. Рис. 1.2(а)) наведено підсумкове зображення після згладжування, ДКП, селекції коефіцієнта та формування масиву серій ОБ, а на другому рисунку наведено зображення-синтетик з маркованими яскравістю (×100) ОБ сформованих серій (див. Рис. 1.2(б)), щоб побачити, як же само розташовуються ОБ зображень в підсумковому зображенні [6]. При низькому рівні візуальної помітності внесених спотворень, помітно розширена область покриття однаковими фрагментами, що є вкрай корисною властивістю для подальшого формування масиву серій ОБ та скорочення процедур проведення ДКП.

а)



б)

Рисунок 1.2 – Результат «збірки» контейнера типу «портрет» за результатами виконання 3-х етапів тестового алгоритму (ОБ 16×16 ел.)

Даний приклад підтверджує мале демаскування контейнера, підготовленого для інкапсуляції контенту, при зниженні загальної обчислювальної складності, що є істотним для мобільних платформ. На рисунку 1.3 представлено варіант відновлення контенту зі зміщенням ОБ всього лише на одну серію. Цей випадок еквівалентний спробі несанкціонованого підбору лише одного параметра ключа – «розміщення ОБ контенту» в умовах деактивації всіх інших параметрів обробки в «Лайт» версії алгоритму, як демонстратор можливостей загальної концепції [1].

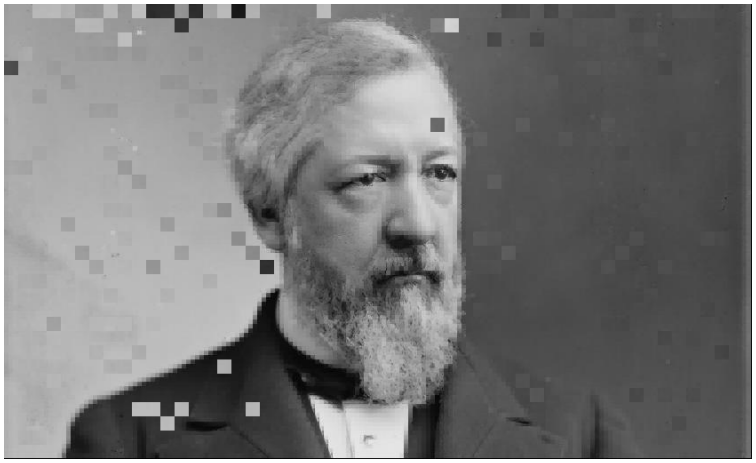


Рисунок 1.3 – Результат хибного вилучення контенту при зсуві ОБ на одну позицію

Характерні залежності кількості ОБ, що формуються, від типу зображень і параметрів (розмір блоків і P_Z) з обробкою та без, представлені на рис. 1.4, 1.5.

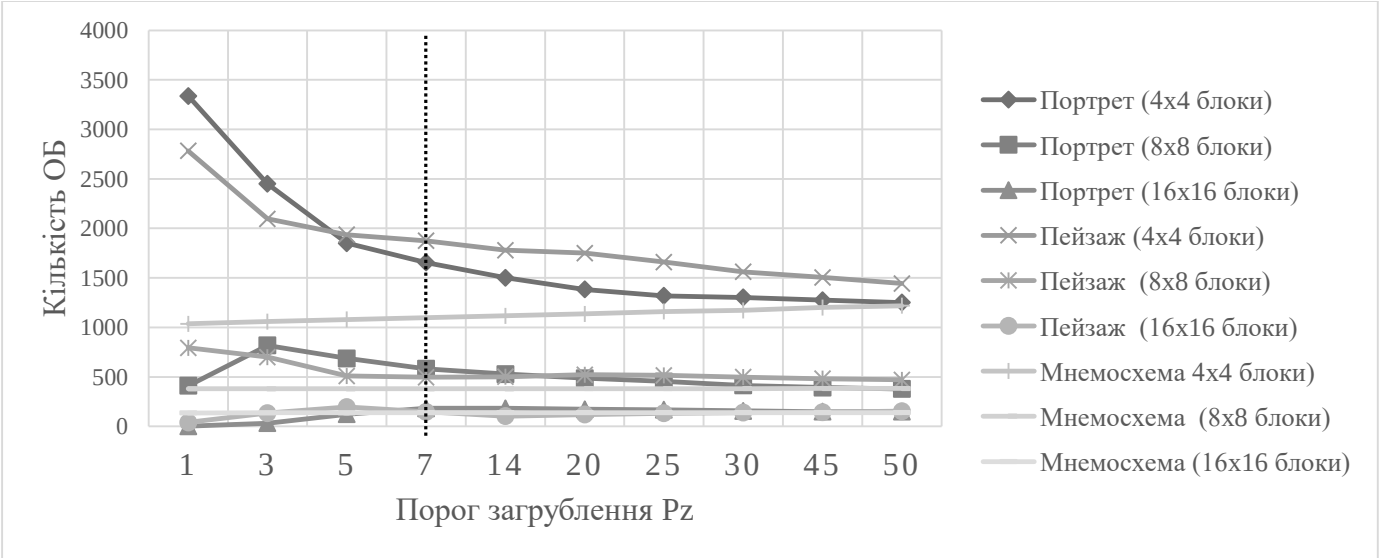


Рисунок 1.4 – Кількість ОБ різної розмірності, зображень та P_z (з обробкою)

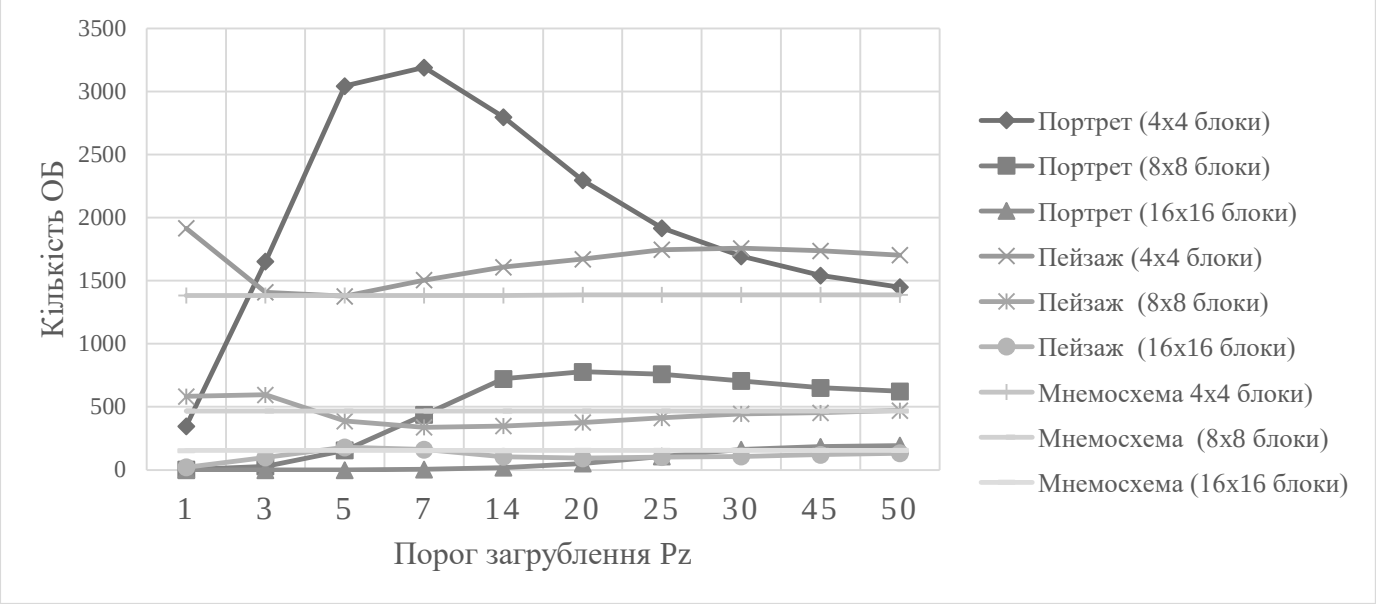


Рисунок 1.5 – Кількість ОБ різної розмірності, зображень та P_z (без обробки)

На рис. 1.6 представлені характерні значення часу виконання 1-го етапу алгоритму для двох розмірностей згладжування масок (3×3 та 5×5 ел.) при різних варіантах передобробки вхідних даних і різних значеннях P_Z [1,2].

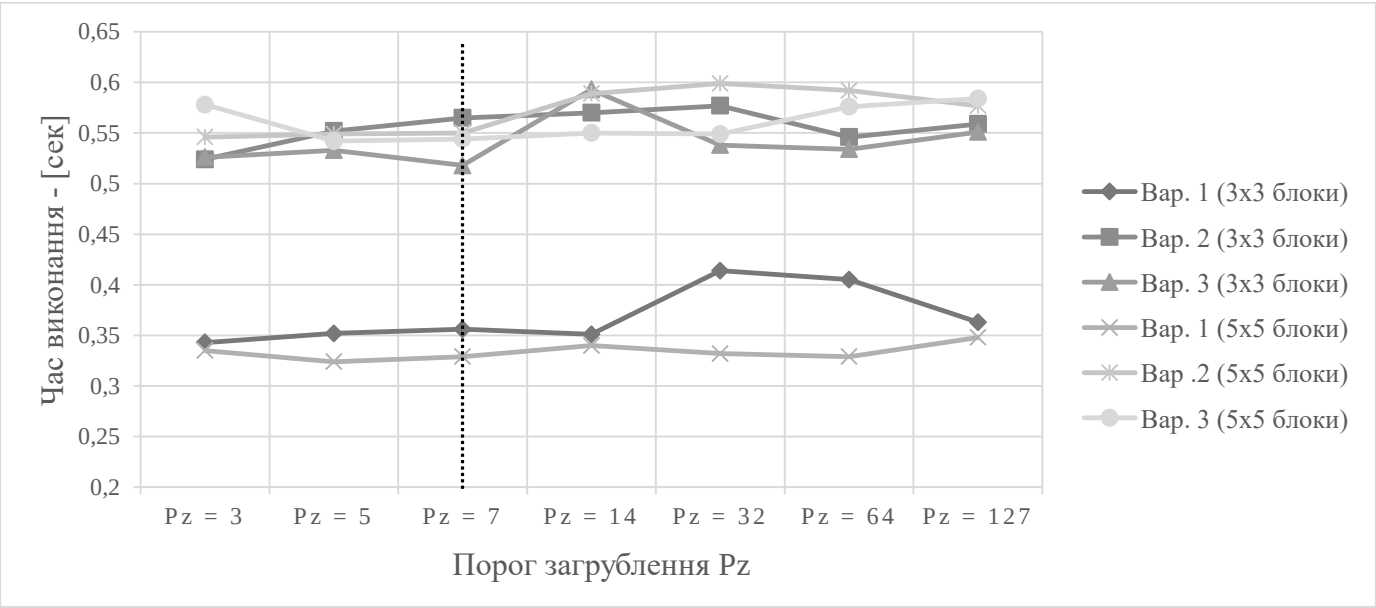


Рисунок 1.6 – Час виконання варіантів для масок різної розмірності

Залежність величин спотворень середньоквадратичної помилки (СКП) та пікового відношення сигнал-шум (PSNR) контейнерів, що утворюється для різних типів зображень і варіантів передобробки вхідних даних при зміні значення порога загрублення сусідніх елементів зображень (P_Z), представлені на рис. 1.7, 1.8.

У всіх чотирьох випадках (рис. 1.4, 1.6, 1.7, 1.8) вертикальний пунктир (на рівні $P_Z = 7$) позначає межу візуальної помітності спотворень сусідніх елементів.

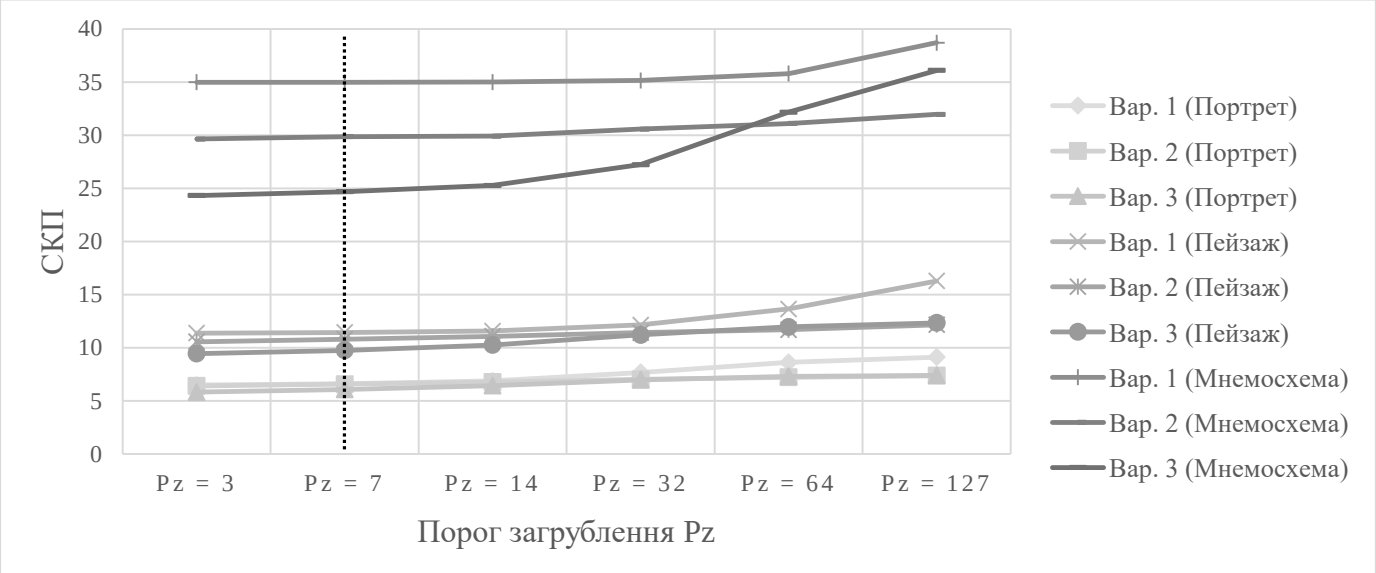


Рисунок 1.7 – Залежність СКП від P_Z для різних типів зображень (маска 5×5 ел.)

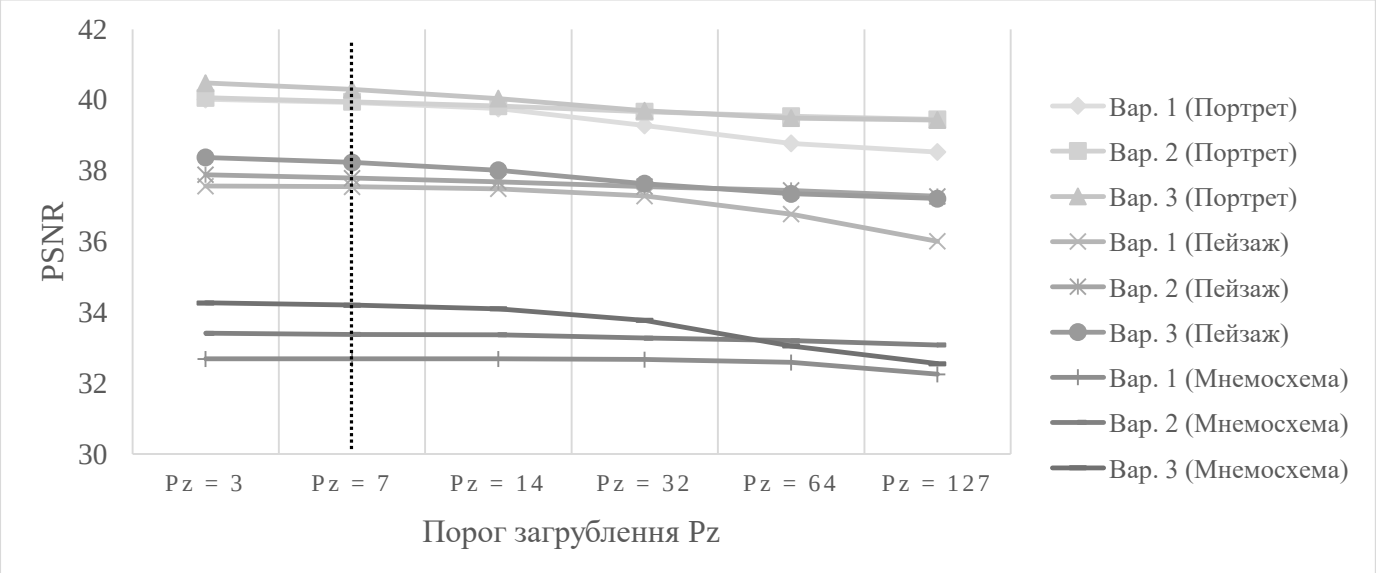


Рисунок 1.8 – Залежність PSNR від P_Z для різних типів зображень (маска 5×5 ел.)

Застосування для обробки контейнера та контенту різних варіантів попередньої обробки та/або різних настановних параметрів алгоритму (наприклад, розмірність блоків та P_Z), сприяє створенню необхідних стартових умов для покращення характеристик формування серій з блоків з однаковим змістом [1,2]. Кількість серій, що формуються, залежить від типу зображень, параметрів їх розмірності та згладжування, що використовується (варіанту передобробки) [4].

Зменшення загальної кількості блоків зображень (контейнера та контенту), що вимагають проведення прямого та зворотного перетворень (у даному випадку двовимірного ДКП), забезпечує скорочення часу обробки та сприяє зниженню обчислювальної складності всього алгоритму.

Використання етапу попередньої обробки вхідних даних, незалежно від його процедурних особливостей, дозволяє помітно збільшити довжину серій ОБ, що значно знижує обсяг необхідних обчислень на етапах проведення кодування з перетворенням.

Так, наприклад, для матриць розмірністю 8×8 елементів, в діапазоні значень порога загрублення яскравості (P_Z) від 5 до 7 градацій (тобто в області малої помітності спотворень), різниця в кількості ОБ може становити мінімум 1,5-2 рази [4].

Причому, залежно від специфіки процедур використовуваного варіанта передобробки вхідних даних [2,6], різниця в кількості ОБ, що формуються, може бути ще більш істотною - майже в 5 разів [4].

Збільшення розмірності блоків фрагментації вихідних зображень, очікувано призводить до помітного зменшення загальної кількості формованих серій ідентичних блоків (тобто ОБ), незалежно від реалізованих варіантів попередньої обробки вихідних даних (див. Рис. 1.4, 1.5).

Для всіх варіантів передобробки, збільшення порога загрублення яскравості сусідніх елементів, більш ніж на 15 градацій (у більшості випадків, це фактично верхня межа порога візуальної помітності спотворень), не призводить до подальшого збільшення довжини серій, ідентичних за вмістом блоків. Тобто, загальна кількість блоків, які потребують проведення перетворень на 3-му етапі алгоритму,

стабілізується в певних межах. Цей ефект характерний для всіх розмірностей субблоків, у всьому «верхньому» діапазоні значень P_Z (від 15 до 50) [4].

При цьому слід відзначити наявність суттєвих відмінностей у кількості ОБ, що формуються, при використанні різних способів передобробки.

Для різних типів тестових зображень характер отриманих залежностей, в цілому, зберігає загальні тенденції. Наявні відмінності обумовлені суттєвою різницею у структурі тестових зображень різного типу (насамперед середнього значення ймовірності перепаду яскравості між сусідніми елементами зображень).

З точки зору покращення стартових умов для наступного здійснення стегановставки, найбільш цікавим є діапазон загрублення яскравості «P_Z» від 3 до 8 градацій. Саме у цьому діапазоні спостерігається різке зростання кількості ОБ, що формуються. Причому для малих субблоків з однаковою розмірністю (8×8 та 16×16 ел.) це зростання найбільш очевидне [4].

Варіюючи розмірністю маски згладжування і типом контейнера можна забезпечити необхідний компроміс, між допустимим ступенем спотворень контейнера і кількістю ОБ, що, в подальшому, забезпечує потрібну комбінаторику використовуваних рівнів мультиплексу даних, де кожен з рівнів визначає свою позицію в структурі складового ключа екстрактора даних.

Тестова версія дослідного алгоритму реалізує 2-х рівневу обробку даних для реалізації стегановставки:

1) міжблокове перенесення даних (між діючих пар параметрів сформованих серій ОБ) [8,11];

2) внутрішньо блокове перенесення даних (між кожного з ОБ) [9,15].

Параметри довжин серій ОБ та фактична кількість ОБ контейнера є одними з головних елементів у структурі складеного ключа екстрактора даних [1].

Виходячи з поточних характеристик зображення-контенту, можливо оперативно змінювати властивості наявних контейнерів (наприклад, що є в пам'яті мобільного пристрою).

2 ДОСЛІДЖЕННЯ МЕХАНІЗМІВ СИНТЕЗУ СКЛАДЕНОГО КЛЮЧА ЕКСТРАКТОРА

Як було зазначено в Розділі 1, основна ідея процедур четвертого етапу полягає, у безпосередньої інкапсуляції даних контенту до масиву ОБ зображення контейнера.

Для цього процедури 4-го етапу [2] мають багаторівневу реалізацію, де кожен із рівнів визначає свою позицію у структурі композитного ключа екстрактора даних [1,7]. В рамках даної роботи досліджені процедури обробки даних, кожна з яких формує 4 із 6-ти (передбачених обраною концепцією) позицій в загальній структурі складового ключа екстрактора даних.

Загальна парадигма створення ключа екстрактора, дозволяє співвідносити діючий стан його елементів із вмістом реалізованих процедур обробки на всіх етапах дослідного алгоритму, що і забезпечує можливість легітимного вилучення контенту.

Головним завданням, умовно 1-го елементу ключа екстрактора (порядок розміщення відповідних ключових елементів, теж складає відповідну позицію), є визначення розмірності ОБ зображення-контейнера. Для формування масиву ОБ зображення-контенту, використовується перший етап алгоритму (попередньої обробки - згладжування), в межах якого виконується зменшення кількості візуально малопомітних перепадів яскравості елементів вихідних зображень за рахунок згладжування їх малоінформативних областей [2,19,20].

У ході дослідження було визначено, що на етапі згладжування, найкращим показником є матриця округлення з розмірністю 3×3 та 5×5 ел., оскільки такі розмірності зменшують величину спотворень вихідних даних.

При розмірностях вікна матриць згладжування більш ніж 5×5 елементів, виникає розмноження помилок в зображенні (якість зображення погіршується і виникають артефакти), а кількість отриманих ОБ не значно зростає. Основним

пріоритетом при виконанні процедур 1-го етапу, є забезпечення балансу між кількістю одержуваних серій ОБ, та якістю та якістю формованого зображення [4,6].

Також, слід підкреслити, що значення розмірності вікна матриць згладжування і значення P_z першого етапу алгоритму, не входять в структуру ключа екстрактора, проте вони здійснюють безпосередній вплив на характеристики одержуваного базового масиву серій ОБ [4].

Основним призначенням 2-го ключового елементу є визначення діючого способу організації розгортки серій ОБ.

Після формування базового масиву серій ОБ, використовуються різні способи їх розгортки. Зміна способу розгортки імітує різні стани елемента складеного ключа екстрактора даних, що визначає діючий принцип формування масиву серій ОБ.

Використання різних способів розгортки серій та порядку вибірки діючих пар параметрів серій ОБ та/або їх окремих компонентів, в рамках реалізованого способу розгортки, забезпечує досить широке комбінаторне поле, значно «посилюючи» роль даного елемента в загальній структурі ключа екстрактора даних [7,9].

Основним призначенням 3-го та 4-го елементів є посилання на дійсний варіант маски мультиплексу діючих параметрів серій ОБ на першому рівні (міжблочному) мультиплексування даних та, відповідно, маски зсуву (перемішування) поточних значень середньої яскравості ОБ контенту (елементів трансформант з координатами (0; 0), [11,19]), на другому (внутрішньоблоковому) рівні мультиплексування [9].

У рамках запропонованої концепції гібридного стеганоалгоритму [1] до структурі композитного (складеного) ключа екстрактора даних входять ще два елементи, які на даному етапі робіт з алгоритмом, не були розглянуті, а саме:

– визначення ознаки симетрії обробки даних контенту та контейнера. В рамках проведеного моделювання було досліджено тільки симетричний режим [1];

– визначення номеру дійсної маски інкапсуляції (стегановставки) даних зображення-контенту безпосередньо в блоки зображення-контейнера. Цей елемент визначає 3-й рівень мультиплексування даних, вже на рівні зображення-контейнера.

Структура ключа екстрактора, що відображає загальну концепцію гібридного стеганоалгоритму [1], в його діючої версії [7,9], представлена в таблиці 2.1.

Таблиця 2.1 – Структура та опис елементів прототипу ключа екстрактора даних

Позиція ключа	**Зміст процедур**	**Комбінації, що моделюються**
1	Розмірність ОБ для зображення-контейнера	4-8-16
2	Діючий спосіб організації розгортки серій ОБ	Розгортка по стовпчикам;
		Розгортка по рядках
		Розгортка «Змійка»
3	Маска перестановок діючих параметрів серій ОБ на 1-му рівні (міжблочному) мультиплексуванні вхідних даних	Короткий стек
		Довгий стек
4	Маски перестановок діючих значень (0; 0) для всіх на 2-му рівні (внутрішньоблочному) мультиплексуванні вхідних даних	Короткий стек
		Довгий стек
5	Визначення ознаки симетрії обробки даних контенту та контейнера	Симетричний режим
		Несиметричний режим (відключено, не моделювався)
6	Маска інкапсуляції контенту у контейнер	Відключено *(не моделювався)*
6+	Комбінація розміщення ключових елементів №№ 1-5	Остання складова при визначенні ВСІХ активних позицій *(не моделювався)*

Таким чином, на момент виконання досліджень. в загальну структуру складового ключа екстрактора даних входять 6 основних (процедурних) елементів, з них: - 4 активні (тобто ті, зміна стану котрих моделювалась), та 2 відключені (зміна їх станів не моделювалася).

Компонент «6+» (див. Табл. 2.1), не пов’язаний з будь-якими спеціальними процедурами обробки контенту, а лише розширює комбінаторику структури самого ключа, тому його використання на даному етапі робіт не розглядалося, але його присутність повинна бути зазначена.

Діюча позиція ключа №1 передбачає наступні комбінації розмірності ОБ: 4×4, 8×8 та 16×16 ел. Використання інших розмірностей не є доцільним за рядом причин [4], що обумовлено кінцевим призначенням алгоритму, що розробляться.

Позиція ключа №2 містить три варіанти розгортки (комбінації): 1 - (Розгортка по стовпцях); 2 - (Розгортка по рядках); 3 - (Розгортка «Змійка») [7].

Позиції №3 та №4 містять дві комбінації мультиплексування вхідних даних, котрі реалізуються на різних рівнях обробки даних (міжблочному та внутрішньоблочному): 1 - Короткий стек; 2 - Довгий стек [7,9,11,24].

Позиція №5 визначає ознаку симетрії обробки даних контенту і контейнера, де за замовчуванням, в межах даної роботи,, використовується симетричний режим.

Позиція №6 визначає використовуваний варіант маски інкапсуляції (стегановставки) контенту на 3-му рівні мультиплексу. Зміна станів цього елементу, на даному етапі робот, не моделювалась.

Також варто зазначити присутність другого шару обробки [1], локалізованого у межах виключно блоків контенту [17]. Однак такий мультиплекс слід розглядати, як додатковий рівень підвищення скритності, з дещо обмеженим діапазоном взаємних перестановок, з усіма наслідками.

Загальна структура ключа екстрактора даних, що притаманна для умов реалізації вище зазначених рівнів обробки даних, відображена на рис. 2.1 [1].

Таким чином, одночасне використання різних комбінацій параметрів обробки даних контенту, що пов’язані з відповідними елементами ключа екстрактора, дозволяє отримати більш суттєвий ефект, з точки зору посилення можливостей алгоритму, щодо протистояння спробам злому (неавторизованого вилучення) контенту [7,8,9].

Додавання до структури ключа рівня 6+ (табл. 2.1) додатково підсилює стійкість ключа до підбору діючих параметрів стегановставки.

Неправильний підбір (злом) дійсної позиції ключа, приносить в загальний результат «свої» руйнівні наслідки, що наочно підтверджується результатами атаки даних, навіть на короткому стеку вибірки [8,15].

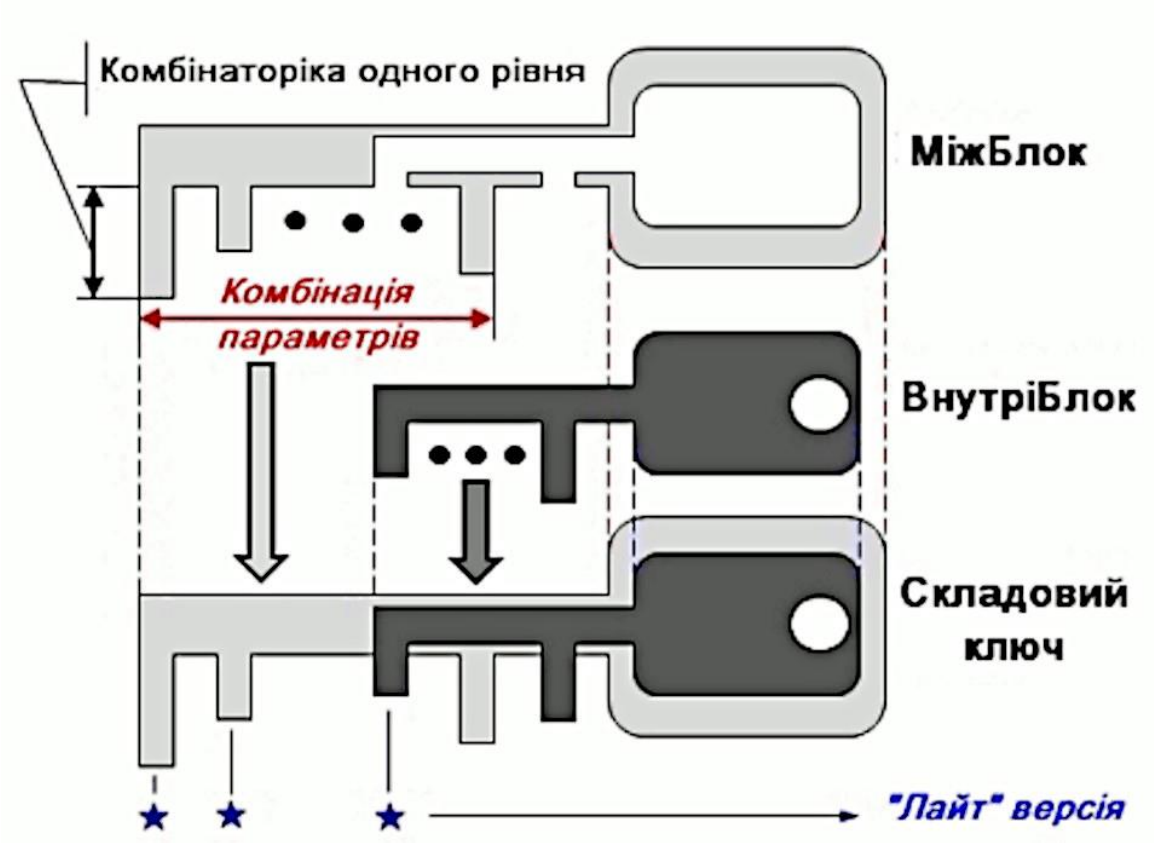


Рисунок 2.1 – Спрощена схема синтезу складового ключа екстрактора

3 ФОРМУВАННЯ СТРУКТУРИ КОНЦЕПТУ ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ БАГАТОРІВНЕВОГО МУЛЬТИПЛЕКСУ ДАНИХ

3.1 Організація розгортки серій ОБ

Фахівцям у галузі обробки зображень добре відомий метод кодування довжин серій, який відрізняється простотою реалізації та має малу обчислювальну складність.

Його використання в системах стиснення відеоданих і форматах представлення графічної інформації, дозволяє отримати хороші результати при обробці зображень, що мають обмежену колірну або яскравість палітру (напівтонові зображення), та/або містять протяжні фонові області з більш-менш однорідною заливкою [11,16,19-21].

Враховуючи специфіку зорової системи людини і особливості методу кодування довжин серій при обробці зображень з різними статистичними характеристиками [11,16,19,20,23], зроблено припущення про можливість його використання для забезпечення процедур міжблокового мультиплексу даних, в рамках обраної концепції реалізації малоресурсного гібридного стеганоалгоритма [1].

Така можливість обумовлена наявністю 3-х важливих обставин, характерних для даного методу:

1) невимогливістю до апаратних ресурсів (орієнтування на мобільні гаджети);

2) високою швидкістю обробки (підтримка режиму реального часу);

3) створенням умов для реалізації процедур міжблокового перенесення окремих параметрів довжин серій ОБ, як інструменту протидії спробам несанкціонованого вилучення контенту.

Процедури міжблочного мультиплексу параметрів серій, передує етапу кодування з перетворенням [11,19,20] для всіх ОБ зображення-контенту [1], що скорочує загальний час роботи алгоритму.

Міжблочний рівень мультиплексування даних забезпечується декомпозицією вихідного масиву ОБ і відповідних значень довжин серій ОБ, за допомогою взаємних перестановок цих елементів в рамках поточної комбінаторики маски перемішування. Кількість і довжина формованих серій ОБ залежить від:

- реалізованого способу згладжування вихідних зображень і порогового значення різниці «P_z» між елементами блоків зображень [1];

- заданої розмірності блоків на етапі формування масиву серій [4];

- статистичних характеристик і типу зображення-контенту [8,11,16,20,23].

Важливо підкреслити, що крім обраної розмірності блоків, найважливішим параметром, що забезпечує легітимацію процедури вилучення контенту, є використовуваний спосіб організації розгортки серій.

Під терміном «розгортка», в даному контексті, слід розуміти спосіб обходу, та наступний порядок вилучення поточних параметрів серій ОБ з базового масиву серій зображення-контенту [12].

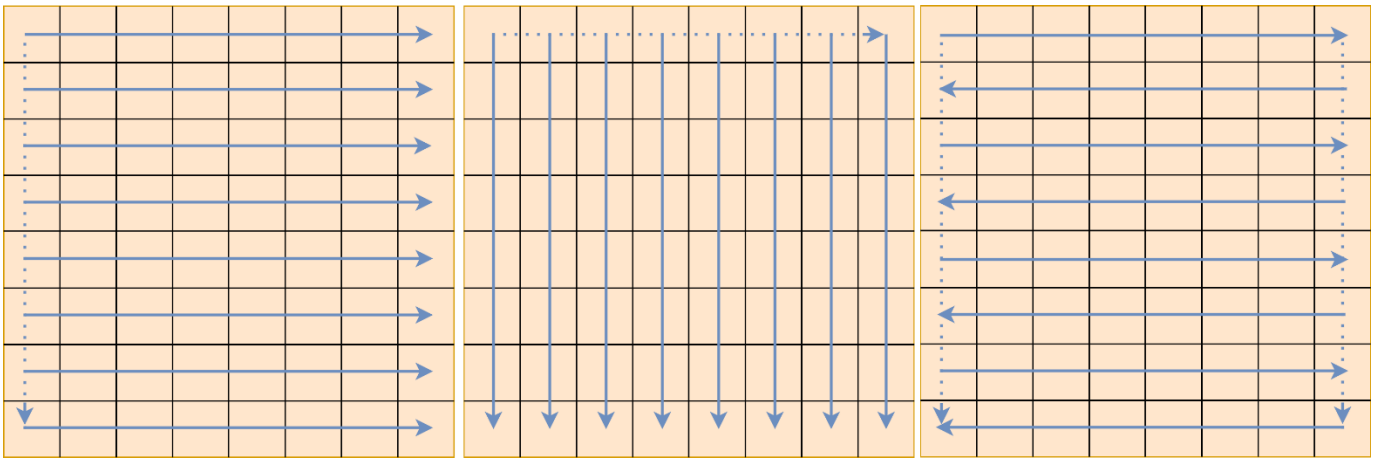
Ці обидва параметри є елементами складеного ключа екстрактора даних, і визначають порядок реалізації процедур кодування-декодування контенту на рівні міжблочної обробки відеоданих-контенту.

Діючий спосіб організації розгортки серій ОБ імітує різні стани елемента складеного ключа екстрактора даних, що визначає принцип формування масиву серій ОБ. Використання різних способів розгортки серій і вибірки діючих пар параметрів (ОБ + довжина серії, [11,19,21]) або їх окремих елементів, в рамках діючого способу розгортки, формують досить широке комбінаторне поле, «підсилюючи» роль даного елемента в структурі ключа екстрактора даних.

На рис. 3.1 представлені тестові (тобто, що моделювались) варіанти реалізації розгортки серій ОБ для діючого релізу алгоритму: 1 − послідовний (ліворуч-праворуч) обхід по стовпцях; 2 − послідовний (згори-вниз) обхід рядками; 3 − зустрічно-зворотний обхід по рядках (т.з. змійка). Використання різних способів організації розгортки серій ОБ і способів вибірки його окремих складових (ОБ або довжини ОБ)

формують ще окрему позицію (див. Табл. 2.1) в загальній структурі комбінованого ключа екстрактора даних [7].

Крім того, можливість комбінування способами вибірки окремих параметрів масиву довжин серій, в рамках чинного механізму розгортки серій, вносить додаткові труднощі в дії атакуючого (в межах даної роботи не розглядається), навіть за умови визначення чинного принципу організації розгортки серій [7].



а) б) в)

Рисунок 3.1 – Способи організації розгортки серій ОБ

Цілком очевидно, що для ускладнення роботи стеганоаналітика необхідно використовувати більш складніші варіанти організації розгортки серій (наприклад, зиґзаґ або спіраль), що більшою мірою руйнують вихідні кореляційні зв'язки між сусідніми серіями ОБ [7]. Тому, запропоновані до уваги варіанти розгортки (по стовпцям, рядкам, змійка) слід розглядати, як демонстратор можливостей, у рамках реалізації основних етапів обробки для діючого релізу прототипу алгоритму.

Тому числі, внесення навіть невеликих змін до способу організації розгортки серій, наприклад, перехід від розгортки рядками до варіанту «змійка», вносить істотні корективи до змісту контенту, що відтворюється [7].

3.2 Міжблоковий рівень мультиплексування даних контенту

Як вже було зазначено вище, міжблоковий рівень мультиплексу даних забезпечує декомпозицію ОБ і відповідних значень довжин серій ОБ за допомогою взаємних перестановок цих елементів у рамках поточної комбінаторики маски перемішування. В рамках даної роботи була використана «Лайт» версія тестового алгоритму, яка обмежена мультиплексуванням 2-х елементів (ОБ та параметра їх довжин серій) складового ключа екстрактора, що формують 1-й рівень комбінаторики параметрів стегановставки.

Для умовного нормування представлених результатів було використано однакові довжину стека вибірки досліджуваних параметрів (відповідно короткий та довгий) та однакові тестові зображення 3-х типів.

Шифрування контенту на короткому стеку, було обмежено послідовністю з 4 серій ОБ. Тестова маска помилкових перестановок (використаних зловмисником для отримання контенту), в рамках одного короткого стеку, представлена на рис. 3.2.

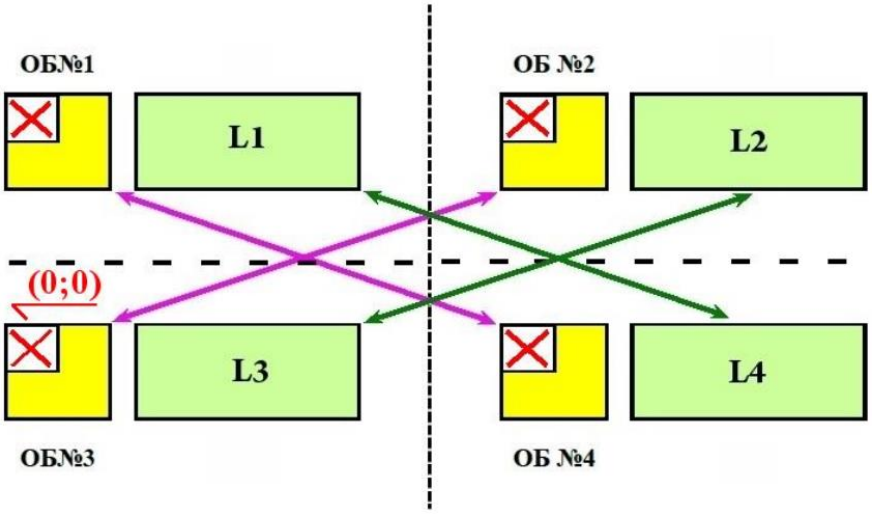


Рисунок 3.2 – Маска перестановок на короткій вибірці [24]

Суть маски перестановок на короткій вибірці (для діючого релізу прототипу) полягає в наступному: - після формування базового масиву серій ОБ, отриманий масив розбивається на 4 підмасиви (тобто, кожен 1-й, 2-й, 3-й та 4 елемент масиву

записується у новий підмасив), в кожному підмасиві виконується перестановка для двох випадків:

1) Маска для заміни ОБ із заданим кроком, виконується перестановка місцями з кроком «2» для 1-го та 4-го ОБ та кроком «1» для 2-го та 3-го ОБ) на циклі з кожної послідовності, що складається з 4-х серій ОБ.
2) Маска для заміни параметра довжин серій із заданим кроком, виконується перестановка місцями з кроком «1» для 1-ї та 4-ї довжини серії та кроком «1» для 2-ї та 3-ї довжини серії.

Якщо отриманий масив серій не укладався в повний цикл (тобто не кратний 4) застосовувалася секретна комбінація для елементів масиву які не були кратні 4. Якщо залишався залишок, то для нього застосовувалося 2 способи: - в першому, решта елементів масиву залишався не зачепленим, тобто після перемішування він додавався в кінець отриманого після перемішування масиву без змін; - другий варіант аналогічний 1-му, але решта елементів розміщені у зворотному порядку.

Вибір стека малої довжини обумовлений припущенням того, що неправильний підбір параметрів вилучення контенту (спроба злому) на стеку з широкою базою призводить до більш руйнівних результатів відновлення вихідних даних. Іншими словами, використання широкої бази перестановок ключових параметрів призводить до більшого порушення просторової кореляції між елементами зображень [3].

Інша тестова маска перестановок параметрів серій, що діють, на довгому стеку вибірки (або, «довгий стек»), представлена на рис. 3.3. Даний варіант перестановки реалізує перемішування: - параметра довжин серій (кожного парного) між двома напівстеками загальної бази, непарним ОБ, між двома напівстеками і решти/рідних параметрів довжин серій (тобто всіх непарних) всередині кожного з 2-х напівстеків.

Суть маски перестановок на довгому стеку вибірки (для діючого релізу прототипу) можна описати трьома етапами.

На першому етапі вихідний масив ділиться на два напівстека (Напівстек А та Напівстек Б). Якщо вихідний масив має лічильну кількість елементів (не кратний 2),

виконується секретна комбінація, в якому останній елемент «непарний» записується в окремий масив і подальші етапи виконуються без нього. Після виконання подальших етапів останній елемент додається в кінець результуючого масиву, якщо масив кратний 2 секретна комбінація не використовується.

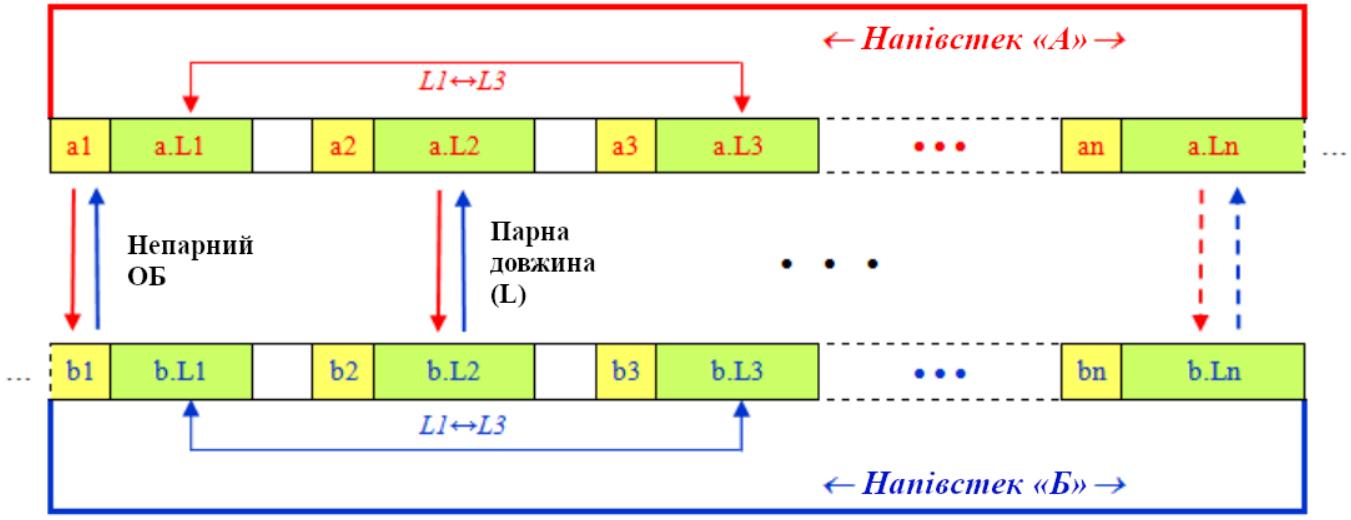


Рисунок 3.3 – Маска перестановок на широкій основі вибірки параметрів серій [7]

На другому етапі виконується перенесення даних (ОБ + L) між двома напівстеками. Кожен непарний ОБ та парна довжина серії в напівстеках А та Б, змінюється між собою місцями.

На третьому етапі виконується попарна рокіровка (перестановка параметра - L) всіх непарних довжин серії в рамках кожного напівстека.

В рамках проведеного моделювання спроб неавторизованого вилучення контенту, передбачалося, що атакуючий зміг правильно визначити поточний параметр довжини стека (тобто базу вибірки) та діючий спосіб розгортки серій, проте помилився у визначенні реалізованого механізму міжблочного мультиплексування відразу для 2-х параметрів (див. Рис. 3.2 - 3.3): - параметра зміщення ОБ (жовті блоки) та параметра довжини серій ОБ (зелені блоки - L).

Причому, припущення, однаково ставилося до умов використання стеків вибірки різної довжини. Відповідно до зазначених припущень розвитку атаки, на

рис. 3.4 представлена візуалізація результатів несанкціонованого отримання тестового контенту, яка характерні для умов використання стеків різної довжини, при різних способах розгортки серій (див. Рис. 3.1).

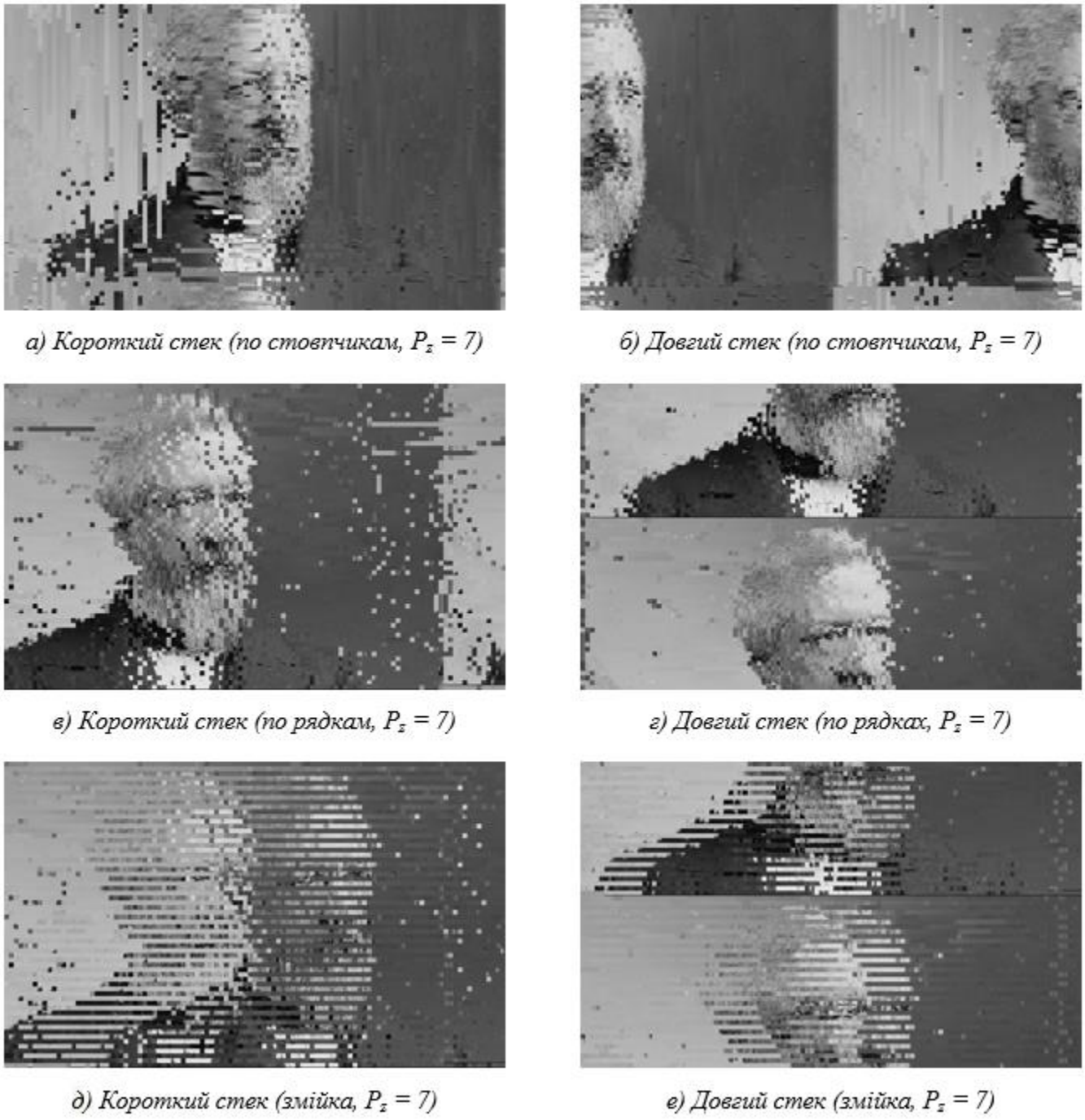
Представлені на рис. 3.4 зразки атакованих зображень дозволяють проявити характерні особливості міжблокового мультиплексу параметрів серій ОБ, як інструменту протидії спробам неавторизованого вилучення контенту.

На представлених зразках добре простежується явна тенденція збільшення дефрагментації вихідних даних при розширенні комбінаторики діючих параметрів серій (тобто при довгому стеку). Окремого коментаря вимагає структура артефактів, характерних для різних способів розгортання серій.

Аналіз атакованих зображень дозволяє стверджувати, що діючий спосіб розгорнення і вибірки параметрів серій (визначається окремою позицією в загальній структурі складового ключа екстрактора даних) значною мірою відбивається на природі артефактів «зламаного» контенту, що візуально фіксуються.

Так, наприклад, порівняння зразків представлених на рис. 3.4 (*а-г*), дозволяє однозначно ідентифікувати характер діючої розгортки (*яку, власне, атакуючий і визначив у рамках прийнятої парадигми експериментального моделювання*), проте не дає уявлення про конкретні параметри діючого способу вибірки окремих параметрів серій в рамках способу, що реалізується. розгортки. До таких параметрів може належати крок вибірки пов'язаних пар (ОБ + довжина, [6,7]) параметрів серій та/або зміна порядку вибірки діючих параметрів залежно від кратності проходу/скану діючого масиву і т.п. У будь-якому випадку цей ключовий параметр вносить серйозні труднощі у дії атакуючого, навіть за умови правильного визначення чинного принципу організації розгортки серій (див. Рис. 3.4).

Важливо мати на увазі, що результати, представлені на рис. 3.4, отримані за умови деактивації механізму внутрішньоблокового мультиплексу даних (2-го рівня), що реалізується в рамках базового масиву серій ОБ після проведення етапу кодування з перетворенням [1,5,7] для всіх ОБ сформованого масиву.



а) Короткий стек (по стовпчикам, P_z = 7)

б) Довгий стек (по стовпчикам, P_z = 7)

в) Короткий стек (по рядкам, P_z = 7)

г) Довгий стек (по рядках, P_z = 7)

д) Короткий стек (змійка, P_z = 7)

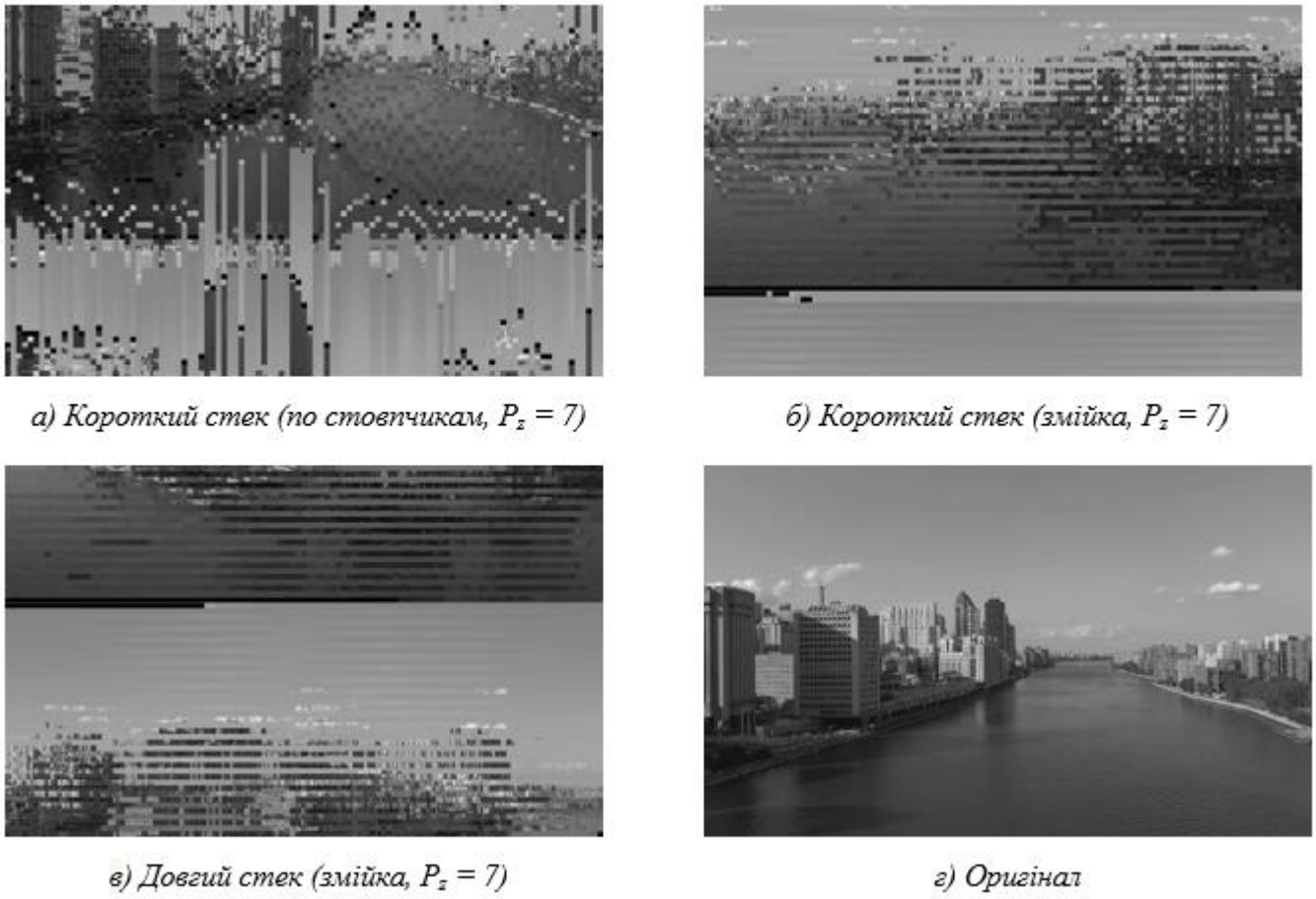
е) Довгий стек (змійка, P_z = 7)

Рисунок 3.4 – Результати атаки тестового зображення типу портрет за різних способів розгортки серій на стеках різної довжини для 1-го рівня обробки

Внесення навіть невеликих змін до принципу організації розгортки серій, наприклад перехід від розгортки по рядках до варіанта «змійка» (див. Рис. 3.4 (*д*,*е*)),

вносить істотні корективи до змісту контенту, що відтворюється, наприклад: − міграції по кадру протяжних областей чорного кольору у високодетальних областях тестового зображення типу «пейзаж» (див. Рис. 3.5, для ОБ 8×8 ел.).

Ця обставина не дає твердих підстав для атакуючого, на успішну фільтрацію несуттєвих (з його погляду) артефактів атакованих зображень, оскільки змушує приймати рішення за умов значної невизначеності щодо вихідної фактури контенту.



а) Короткий стек (по стовпчикам, $P_z = 7$)

б) Короткий стек (змійка, $P_z = 7$)

в) Довгий стек (змійка, $P_z = 7$)

г) Оригінал

Рисунок 3.5 – Приклад міграції протяжних областей чорного кольору по атакованому кадру зображення (*а-в*), залежно від типу розгортки серій ОБ

Таким чином, атакуючий постійно знаходиться в «зоні ризику», яка пов'язана з високою ймовірністю втрати важливих деталей вихідних даних, що істотно змінюють діапазон можливих трактувань сцени, яка спостерігається.

3.3 Внутріблоковий рівень мультиплексування даних контенту

Як вже було зазначалося у попередньому пункті, міжблоковий мультиплекс даних забезпечує декомпозицію вихідного масиву ОБ і відповідних значень довжин серій за допомогою взаємних перестановок цих елементів в рамках поточної комбінаторики маски перемішування (рис. 3.2 - 3.3).

В 1-му випадку використовувався стек завдовжки 4 серії, що зумовлює малу базу взаємних перестановок параметрів серій [4]. А у другому випадку, довжина стека вибірки дорівнювала загальної кількості сформованих серій ОБ, а взаємний мультиплекс параметрів серій здійснювався, як між двома його половинами (напівстеками), так і в рамках кожного з них. В обох випадках проводилося «руйнування» параметрів діючих пар серій ОБ (рис. 3.4 - 3.5) [5].

Основна суть етапу внутрішньоблокового мультиплексування даних полягає у «перемішуванні» значень середньої яскравості ОБ, між всіма матрицями-трансформант ОБ, які були отримані після проведення кодування з перетворенням (в даному випадку ДКП) [20]. Ця процедура, для діючого релізу прототипу, є аналогом 1-го рівня обробки (міжблокового мультиплексу), тобто складається з 2-х тестових масок перестановок (перемішування), що імітують різні комбінації їх складності: - короткого та довгого стеків вибірки значень (0; 0).

В межах роботи моделювалися два різні стани елемента (у загальній структурі ключа екстрактора даних), що відповідає за комбінаторику перемішування 2-го рівня (див. Табл. 2.1 та Рис. 2.1). Таким чином, фактично, імітується різні стани маски перемішування на 2-му рівні мультиплексування параметрів серій ОБ контенту.

Використання внутрішньоблокового мультиплексування даних, доповнює 1-й рівень обробки та розширює можливості протистояння атакам контенту [3,5].

Іншими словами, відповідно до тестової маски перестановок [2], проводиться процедура внутрішньоблокового зсуву всіх коефіцієнтів, що характеризують середню яскравість ОБ. Принцип маски перестановок на короткому стеку вибірці (для діючого релізу прототипу) для внутрішньоблокового перемішування полягає в простій

циклічній заміні елементів (0;0), на періоді в чотири відліки. Тобто виконується взаємне рокірування (перестановка місцями) для 1-го та 4-го ОБ і для 2-го та 3-го ОБ) на циклі з кожної послідовності, що складається з 4-х серій ОБ, тестова маска представлена на рис. 3.6.

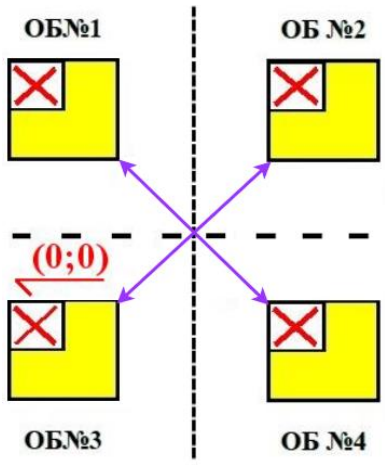


Рисунок 3.6 – Маска зсуву 2-го рівня мультиплексу на короткій вибірці

Сутність процедур синтезу тестової маски перестановок на довгому стеку вибірки (для діючого релізу алгоритму) для внутрішньоблокового рівня обробки можна описати двома етапами.

На 1-му етапі весь отриманий після ДКП масив трансформант ОП ділиться на два напівстека (Напівстек А та Напівстек Б). При цьому, якщо кількість елементів не виходить кратним 2, в даному випадку секретна комбінація не виконується.

На 2-му етапі у першому напівстеку «А» проводиться зворотна (тобто ззаду наперед) перестановка всіх значень (0; 0). В напівстеку «Б» здійснюється взаємна заміна значень (0; 0) у всіх непарних блоках (матрицях коефіцієнта) з кроком через один (тобто 1-й з 3-м, 5-й з 7-м, 9-й з 11-м і т.д), а для всіх парних значень (0;0), виконується зворотна перестановка, як було в напівстеці «А».

Тестова маска перестановок діючих параметрів середньої яскравості ОБ, що реалізовані на довгому стеку вибірки для другого рівня мультиплексування даних, представлено на рис. 3.7.

Таким чином, у кожній половинці напівстека А та Б масиву матриць коефіцієнтів реалізується відразу два різні підходи перемішування «середніх яскравостей ОБ серій». Коротко кажучи в першому напівстеку «А» робиться проста інверсія, без руйнування кореляційних зв'язків параметра яскравості між сусідніми серіями ОБ, а в другому напівстеку «Б» для одних елементів (непарних) стрибаємо через один (роблячи їх рокірування), а для парних, робиться інверсія по всій довжині наявної половинки. Відповідно, у другому напівстеку набагато сильніше руйнуються взаємні зв'язки між яскравістю сусідніх серій.

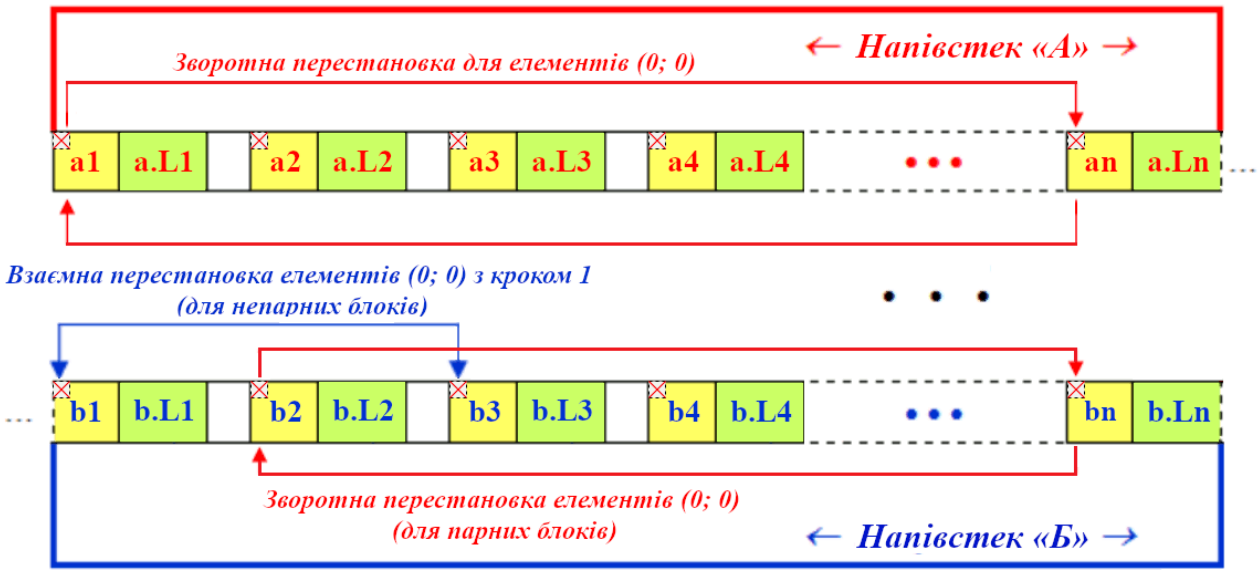
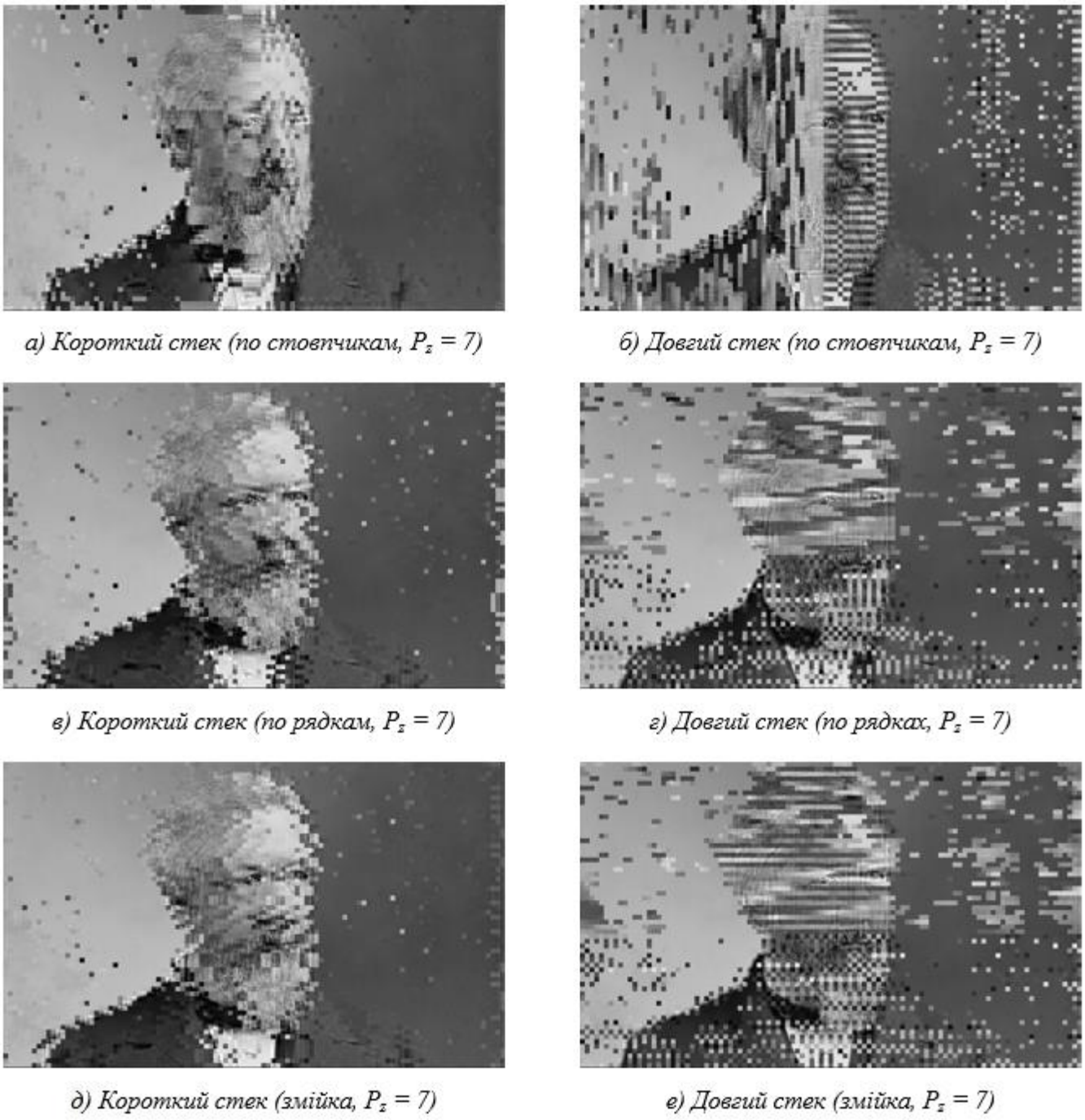


Рисунок 3.7 – Маска перестановок на довгому стеку вибірки

Використання 2-го рівня мультиплексу вихідних даних контенту, слід розглядати, як додатковий рівень, з дещо обмеженим (в порівнянні з 1-м рівнем) діапазоном взаємних перестановок зі всіма наслідками.

В даному разі значною мірою посилюється стійкість контенту до спроб його неавторизованого вилучення, обумовлюючи великі спотворення в оброблюваному зображенні в разі хибного підбору діючих параметрів обробки, чим сильно заважає зловмиснику при спробах несанкціонованої екстракції даних з контейнера. Результати

реалізації процедур внутрішньоблокового мультиплексування даних, для різних способів розгортки серій ОБ, представлені на рис. 3.8 (для зображення типу портрет).



а) Короткий стек (по стовпчикам, $P_z = 7$)

б) Довгий стек (по стовпчикам, $P_z = 7$)

в) Короткий стек (по рядкам, $P_z = 7$)

г) Довгий стек (по рядках, $P_z = 7$)

д) Короткий стек (змійка, $P_z = 7$)

е) Довгий стек (змійка, $P_z = 7$)

Рисунок 3.8 – Результати атаки тестового зображення при різних способах розгортки серій і стеках різної довжини для 2-го рівня мультиплексу (*ОБ розмірністю 8×8)*

3.4 Моделювання режиму дворівневого мультиплексування даних контенту

Як вже було зазначалося у попередніх пунктах, що одночасне використання процедур міжблокового та внутрішньоблокового мультиплексування можуть значною мірою посилити стійкість контенту до спроб його неавторизованого вилучення. Тому, в цьому пункті представлені результати моделювання процедур атаки стеганоконтента, при одночасному використанні процедур дворівневої обробки контенту [15]. Для демонстрації одержуваних ефектів у тестовій версії дослідницького алгоритму було реалізовано вибіркове «відключення» кожного з 2-х передбачених етапів обробки контенту:

1) процедур внутрішньоблокового мультиплексування коефіцієнтів трансформант, що характеризують середню яскравість сформованих ОБ (елементи (0;0)), що отримані за результатами реалізації кодування з перетворенням (ДКП). Тобто, в даному випадку, захист контенту забезпечувався тільки реалізацією процедур виключно на рівні міжблокового мультиплексу;

2) процедур міжблокового мультиплексування поточних параметрів довжин серій ОБ [8]. На рис. 3.9, 3.10 дана операція відповідає блоку «*Multiplex Level 1*» (крок №4). Тобто, в даному разі захист контенту обмежується реалізацією процедур внутриблочного мультиплекса.

Таким чином, на рис. 3.9, 3.10 блок «*Multiplex Level 1*» (крок №4), відповідає режиму міжблокової обробки, а блок «*Multiplex Level 2*» (крок №6), режиму внутрішньоблокового мультиплексування діючих параметрів контенту.

Представлена на рис. 3.9 схема в спрощеному вигляді пояснює загальну сутність процедур, що проводяться на обох рівнях обробки, а рис. 3.10 уточнює режим використання довгого стеку. Коротко розглянемо міст основних процедур.

На 1-му кроці (див. Рис. 3.9) проводиться зчитування вихідних даних.

На 2-му кроці реалізується процедура згладжування вихідних даних [1,4], з використанням встановленого значення порога загрублення (P_z) величини яскравості сусідніх елементів оброблюваних блоків зображення.

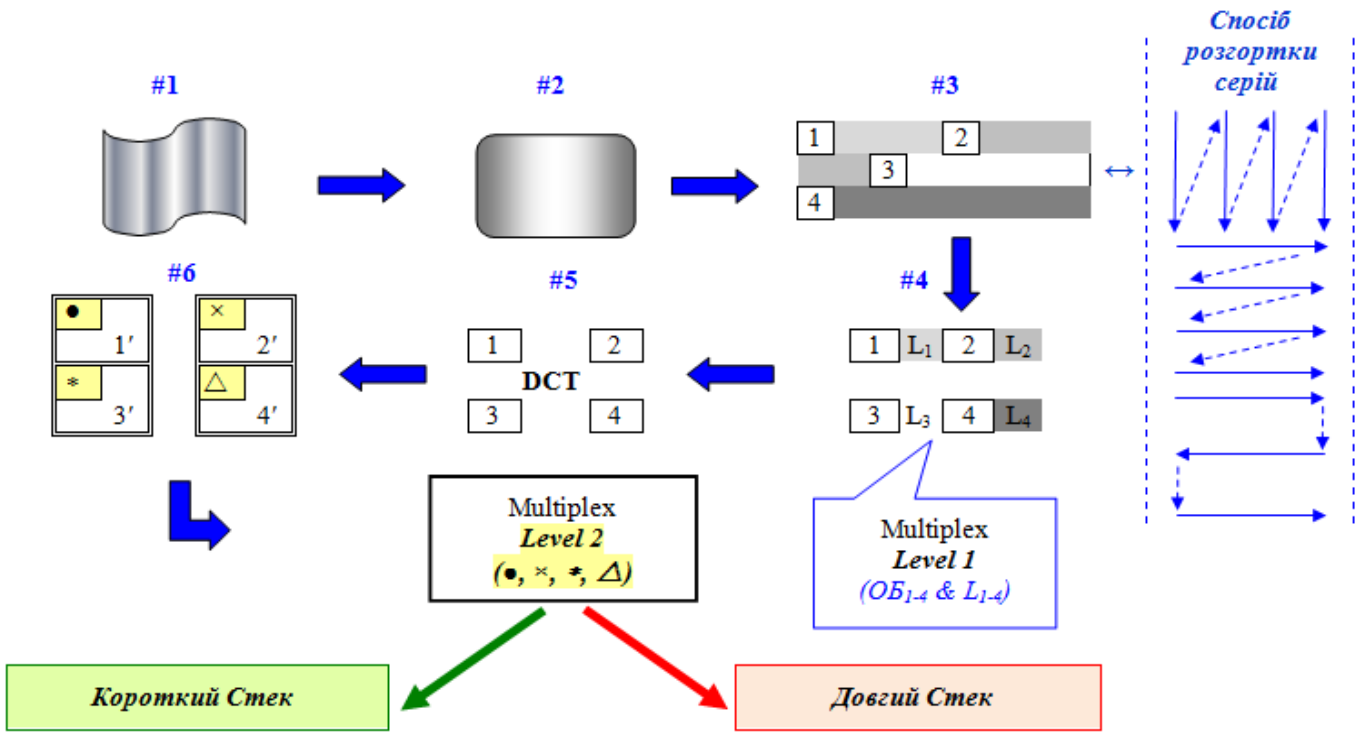


Рисунок 3.9 – Загальна схема процедур дворівневої обробки

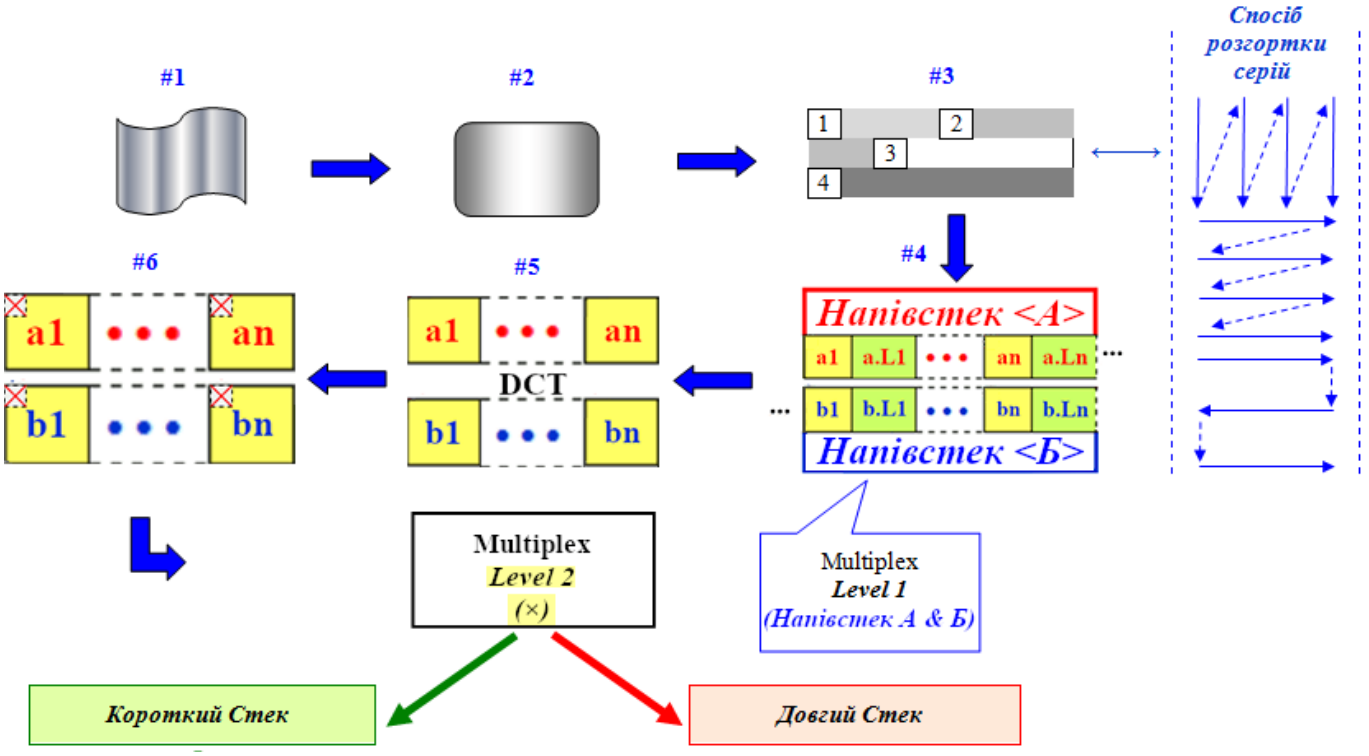


Рисунок 3.10 – Спрощена схема процедур для довгого стеку.

На 3-му кроці виконується обхід «згладженого» зображення вікном (матрицею) заданої розмірності. Визначення серій ОБ зображення-контенту [4], виконується через кодування довжин серій [19,21]. При реалізації даного етапу, порівняння елементів сусідніх блоків зображення проводиться з використанням заданого раніше значення параметру порога загрублення яскравості (P_Z).

На 4-му кроці моделює різні способи організації базового масиву серій ОБ (тобто розгортки серій), що дозволяє імітувати різні стани відповідного елемента в структурі інтегрованого ключа екстрактора даних. У рамках цього етапу, імітуються 3 способи організації розгортки серій: по стовпцях, рядками та «змійка». Після формування базового масиву серій ОБ з використаною розгортки серій виконується сам процес міжблокового мультиплексування для короткого або довгого стеку.

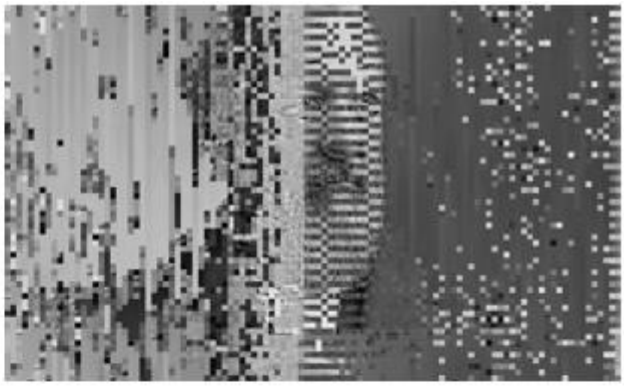
На 5-му кроці алгоритму для всіх ОБ, в сформованому масиві серій, проводиться дискретне косинусне перетворення (*DCT*) [19,20].

На 6-му кроці алгоритму, відповідно до тестової маски перестановок [8], проводиться процедура внутрішньоблокового мультиплексування для всіх коефіцієнтів, що характеризують середню яскравість ОБ. На рис. 3.9, 3.10 елементи (0;0) різних трансформант, позначені символами для короткого стеку (●, ×, *, ⊿), а для довгого стеку (×).

Результати реалізації процедур дворівневого мультиплексування, для різних способів розгортки серій ОБ, представлені на рис. 3.11, 3.12.

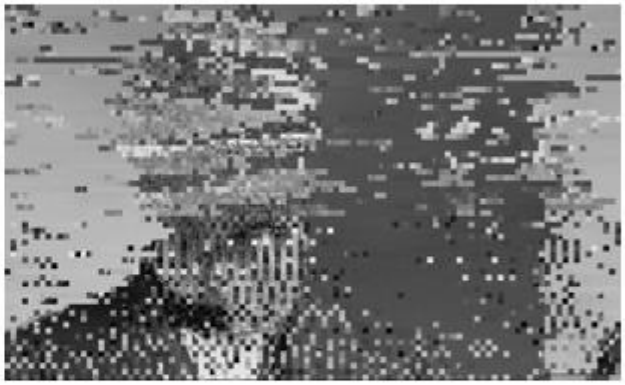
Слід підкреслити, що при моделюванні короткого стеку вибірки серій використовувалась послідовність всього з 4-х серій, а довжина довгого стеку вибірки, дорівнювалась довжині базового масиву серій ОБ, що отримано для вихідних даних контенту [7]. При проведенні даного циклу експериментів на етапах згладжування та формування базового масиву серій ОБ використовувалося значення $P_z = 7$. Такий параметр перебуває у середині області допустимих спотворень сусідніх елементів більшості реалістичних зображень [7,20].

а) Короткий стек (по стовпчикам, P_z = 7)



б) Довгий стек (по стовпчикам, P_z = 7)

в) Короткий стек (по рядкам, P_z = 7)

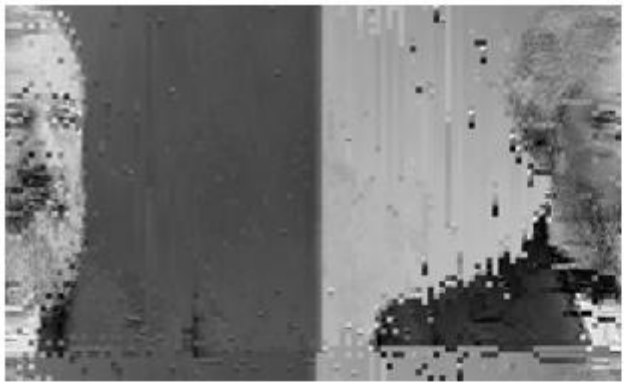


г) Довгий стек (по рядках, P_z = 7)

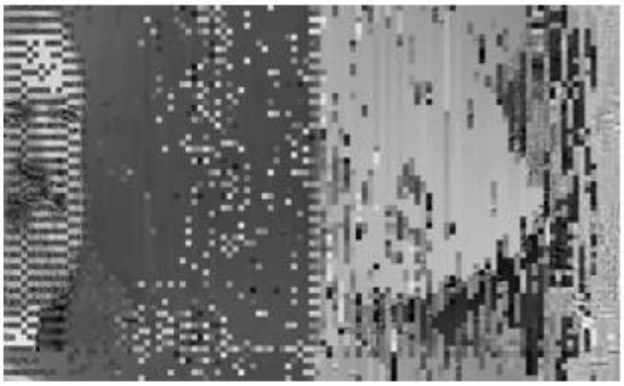
д) Короткий стек (змійка, P_z = 7)

е) Довгий стек (змійка, P_z = 7)

Рисунок 3.11 – Результати дворівневого мультиплексування контенту для короткого стеку *(P_z =7; ОБ 8×8 ел.)*



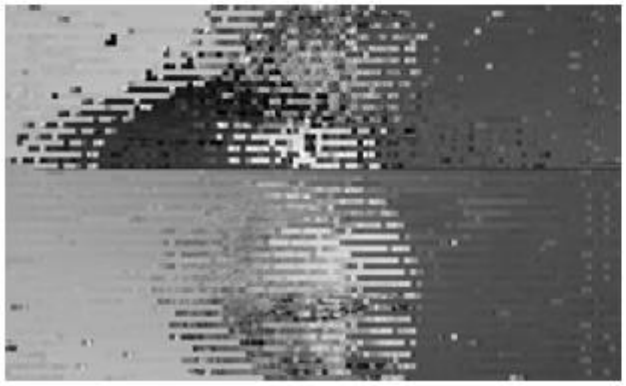
а) Короткий стек (по стовпчикам, P_z = 7)



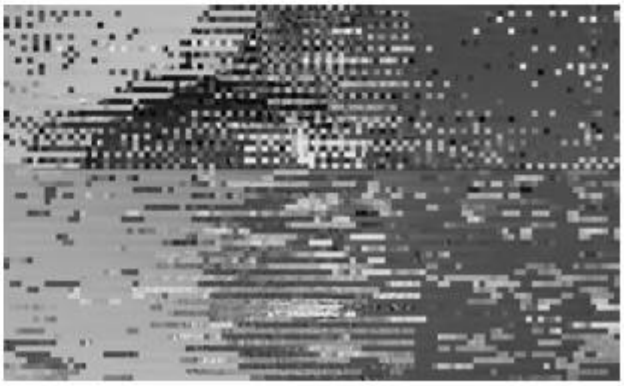
б) Довгий стек (по стовпчикам, P_z = 7)

в) Короткий стек (по рядкам, P_z = 7)

г) Довгий стек (по рядках, P_z = 7)



д) Короткий стек (змійка, P_z = 7)



е) Довгий стек (змійка, P_z = 7)

Рисунок 3.12 – Результати дворівневого мультиплексування для довгого стеку *(P_z =7; ОБ 8×8 ел.)*

Спираючись на отримані результати моделювання [4,7,9,15] можна зробити наступні висновки:

1) Застосування різних способів попередньої обробки (згладжування) контенту дозволяє поліпшити можливу комбінаторику мультиплексу серій, на наступних етапах роботи дослідного алгоритму [1,2,6];

2) Зменшення загальної кількості блоків зображень, що вимагають проведення прямого та зворотного перетворень [1], забезпечує скорочення часу обробки та зменшує загальну обчислювальну складність алгоритму [4];

3) На етапі формування серій ОБ для переважної більшості зображень прийнятним використання розмірностей блоків у діапазоні від 3 до 8 елементів та поріг загрублення $P_Z = 7$, оскільки є оптимальним значенням для переважної більшості різних типів зображень [2]. Використання великих значень призводить до серйозної деградації вихідних даних [10];

4) Збільшення розмірності ОБ для всіх типів тестових зображень призводить до зменшення загальної кількості серій ОБ, що значно звужує базу можливих перестановок для діючих параметрів серій. ОБ з більшою розмірністю, значно меншою мірою схильні тенденції до збільшення числа формованих серій ніж при використанні блоків малої розмірності [4];

5) Використання параметра «довжин серій» ОБ, як один з елементів складеного ключа екстрактора даних, дозволяє отримати набагато більш суттєвіший ефект, ніж при реалізації перестановок тільки за допомогою ОБ [4].

Одночасне суміщення 2-х зазначених параметрів перестановки (ОБ та параметра довжини серій) посилює стійкість контенту до його нелегітимної екстракції. Причому основну роль відіграє параметр довжини серій [11].

6) Використання принципу кодування довжин серій більшою мірою характерне для фонових областей зображень, тому для високоінформативних фрагментів в більшої мірі «працює» 2-й рівень мультиплексування [15,25].

7) Збільшення довжини стека вибірки для діючих параметрів масиву довжин серій (1-й рівень) розширює комбінаторику мультиплексування для обох параметрів сформованих серій ОБ, що значно більшою мірою руйнує кореляційні зв'язки елементів вихідного масиву серій зображення-контенту і тим самим суттєво ускладнює несанкціоноване вилучення та подальшу ідентифікацію вихідного стеганоконтента. Цей ефект гарно підтверджується значним збільшенням щільності розміщення серій різної яскравості, у фонових областях атакованого тестового зображення, що використовує широку базу перестановок [15,24].

8) Опорні блоки та параметри їх довжин серій є основними процедурними елементами на етапі міжблокової обробки контенту (див. Рис. 3.9, крок №4);

9) Розмірність ОБ та різні способи організації розгортки серій (рис. 3.9-3.10) визначають порядок реалізації процедур міжблокової обробки даних і формують відповідні позиції в структурі складеного ключа екстрактора (див. Табл. 2.1);

10) Використання дворівневої обробки контенту (рис. 3.11) вносить серйозні труднощі відносно процесу його ідентифікації (див. Рис. 3.11 - 3.12), навіть за умови визначення чинного принципу організації розгортки серій ОБ;

11) Діючий спосіб розгортки серій, опосередковано визначає структуру артефактів атакованого тестового зображення за умови вдалого підбору одного з діючих механізмів (рис. 3.9) мультиплексування (див. Рис. 3.11 - 3.12);

12) Для ускладнення роботи стеганоаналітика необхідно використовувати більш складніші варіанти організації розгортки серій (наприклад, зиґзаґ або спіраль). При цьому, внесення навіть невеликих змін до принципу організації розгортки серій, наприклад, перехід від розгортки по рядках до варіанта «змійка», вносить істотні зміни до змісту контенту, що відтворюється (*рис. 3.11-3.12 (в-г) проти (д-е)*);

13) Кожен із 2-х використаних рівнів мультиплексування (міжблоковий та внутрішньоблоковий), роблять значний внесок у загальний ефект. Навіть вдалий підбір діючої комбінації, у співвідношенні 2 із 3-х (тобто спосіб розгортки + один із двох рівнів мультиплексу), відчутно руйнує вихідний контент (рис. 3.11 - 3.12).

4 ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТА УЗАГАЛЬНЕННЯ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ ПРОЦЕДУР ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ

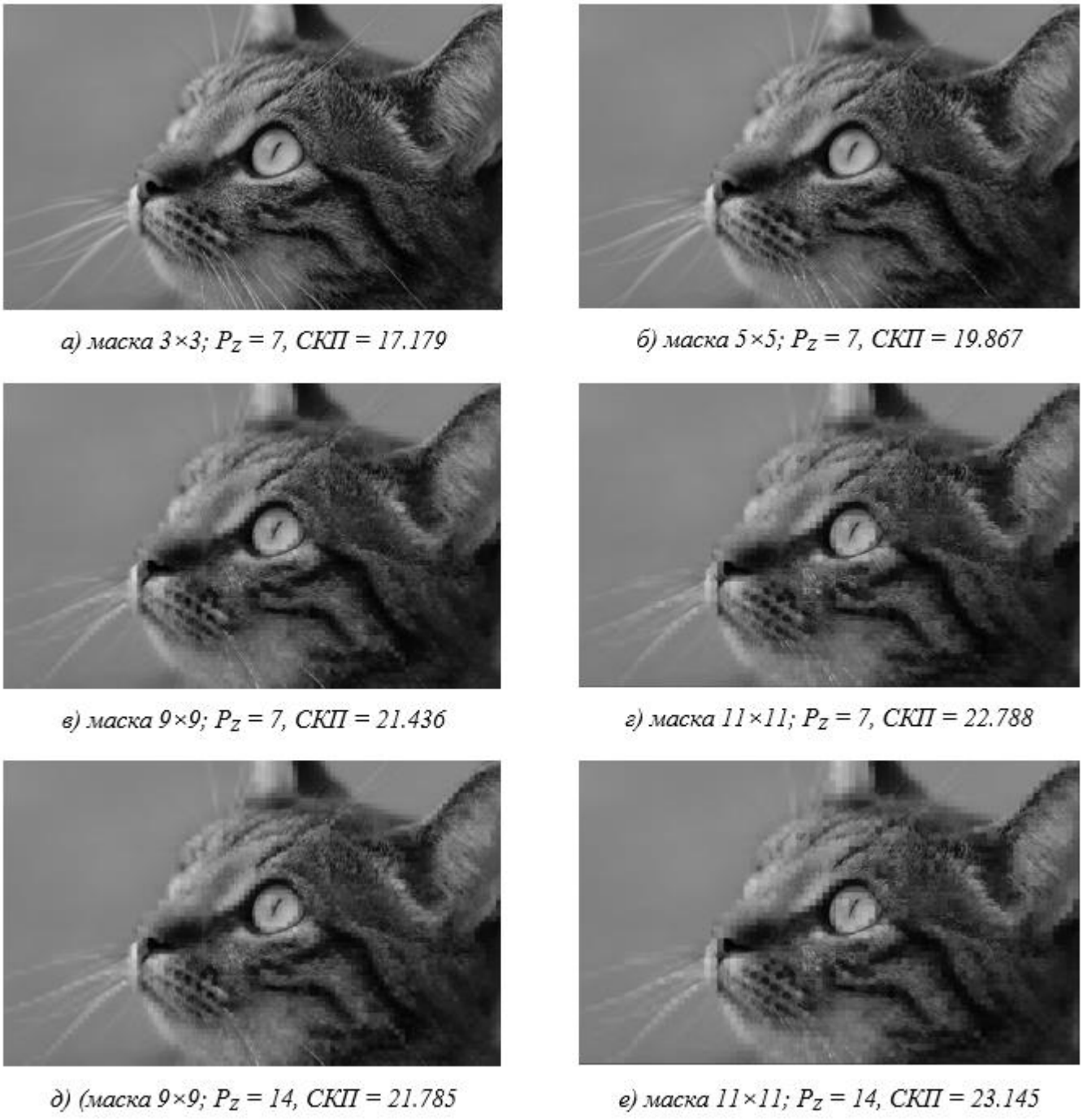
4.1 Визначення граничних параметрів налаштувань для 1-го рівня захисту

У цьому пункті представлені результати моделювання спроб неавторизованого вилучення/атаки стеганоконтента (тестових зразків напівтонових зображень), що захищається за допомогою реалізації міжблокового мультиплексування, з використанням короткого та широкого стека вибірки діючих параметрів масиву довжин серій опорних блоків [1,4,8,11].

У ході моделювання використовуються три різні варіанти передобробки вихідних даних [1], з розміром матриці вікна згладжування 3×3 та 5×5 елементів та подальшим формуванням базового масиву серій ОБ розмірністю 4×4, 8×8, 16×16 елементів, оскільки ці параметри є оптимальними значеннями для етапів передобробки та формування серій ОБ.

Для переважної більшості тестових зображень прийнятним є використання порогу загрублення $P_Z = 7$, оскільки таке значення перебуває в середині області допустимих спотворень сусідніх елементів більшості реалістичних зображень. При цьому, граничним значенням P_Z слід вважати $P_Z = 14$ (для 256 рівнів яскравості), оскільки використання великих значень призводить до серйозної деградації вихідних даних [10], як показано на рис. 4.1, 4.2.

Варіюючи розмірністю маски згладжування контенту і типом зображення контейнера можна забезпечити необхідний компроміс, між допустимим ступенем спотворень контейнера (рис. 4.1, 4.2) і кількістю ОБ контенту, що забезпечує необхідну комбінаторику мультиплексу даних (контенту) в подальшому, на всіх рівнях обробки (рис. 4.3, 4.4).



а) маска 3×3; P_Z = 7, СКП = 17.179

б) маска 5×5; P_Z = 7, СКП = 19.867

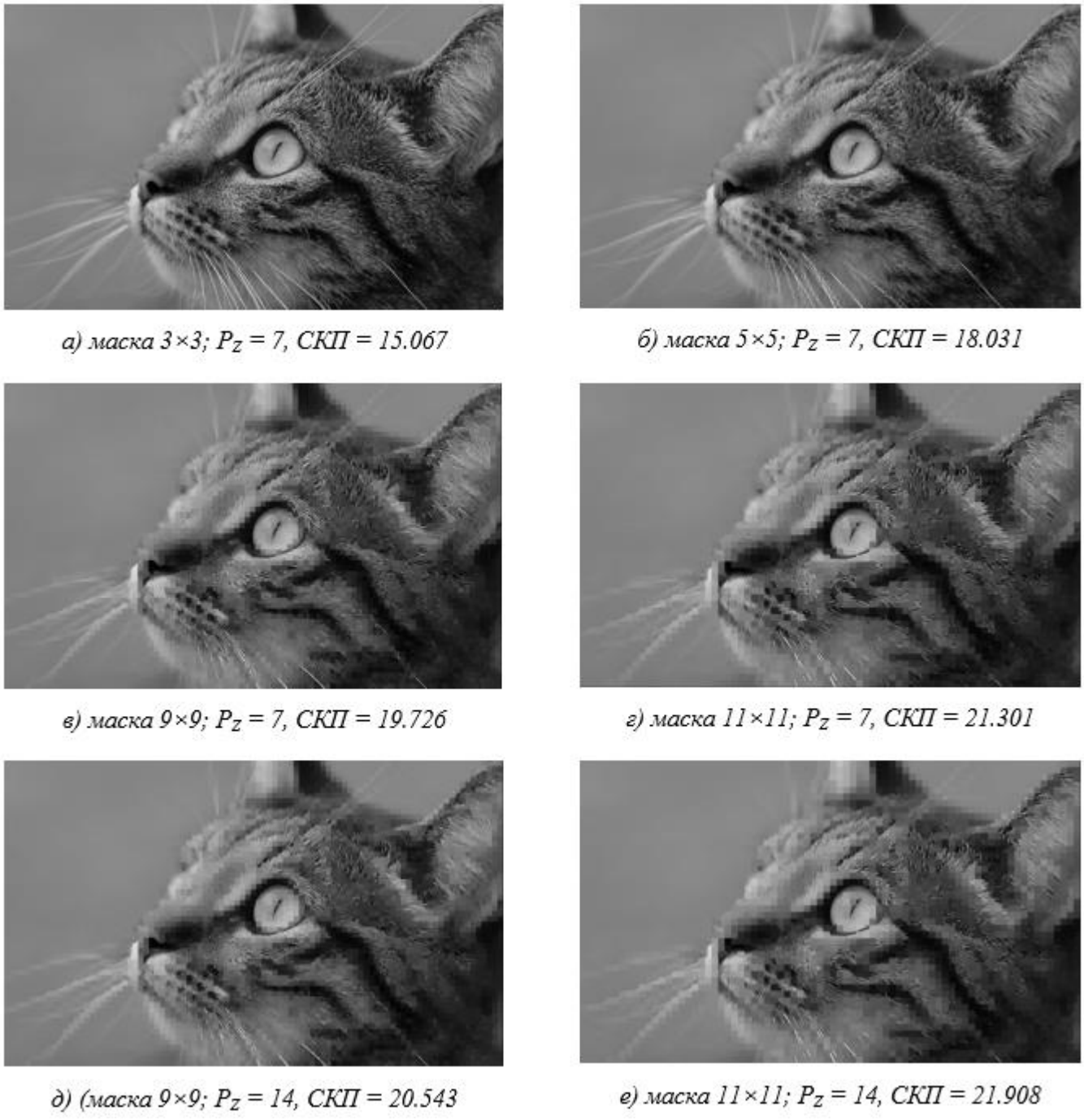
в) маска 9×9; P_Z = 7, СКП = 21.436

г) маска 11×11; P_Z = 7, СКП = 22.788

д) (маска 9×9; P_Z = 14, СКП = 21.785

е) маска 11×11; P_Z = 14, СКП = 23.145

Рисунок 4.1 – Результати застосування 2-го Варіанту передобробки контенту для різних розмірностей маски згладжування та значень P_Z



а) маска 3×3; P_Z = 7, СКП = 15.067

б) маска 5×5; P_Z = 7, СКП = 18.031

в) маска 9×9; P_Z = 7, СКП = 19.726

г) маска 11×11; P_Z = 7, СКП = 21.301

д) (маска 9×9; P_Z = 14, СКП = 20.543

е) маска 11×11; P_Z = 14, СКП = 21.908

Рисунок 4.2 – Результати застосування 3-го Варіанту передобробки контенту для різних розмірностей маски згладжування та значень P_Z

Характерні залежності кількості ОБ, що формуються для зображень типу портрет та пейзаж [19] при різних розмірах блоків та значеннях P_Z, для 3-х варіантів предобробки вхідних даних [2,17], представлені на рис. 4.3, 4.4.

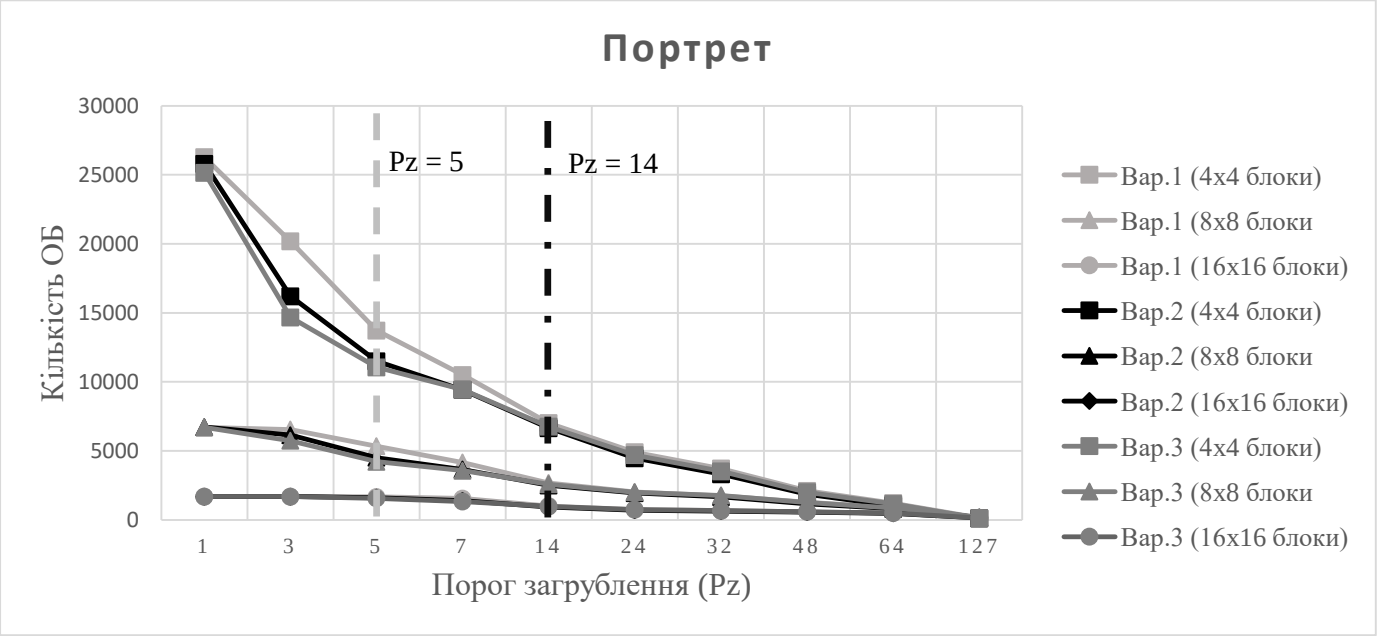


Рисунок 4.3 – Кількість ОБ при різних варіантах передобробки для зображення типу «*Портрет*»

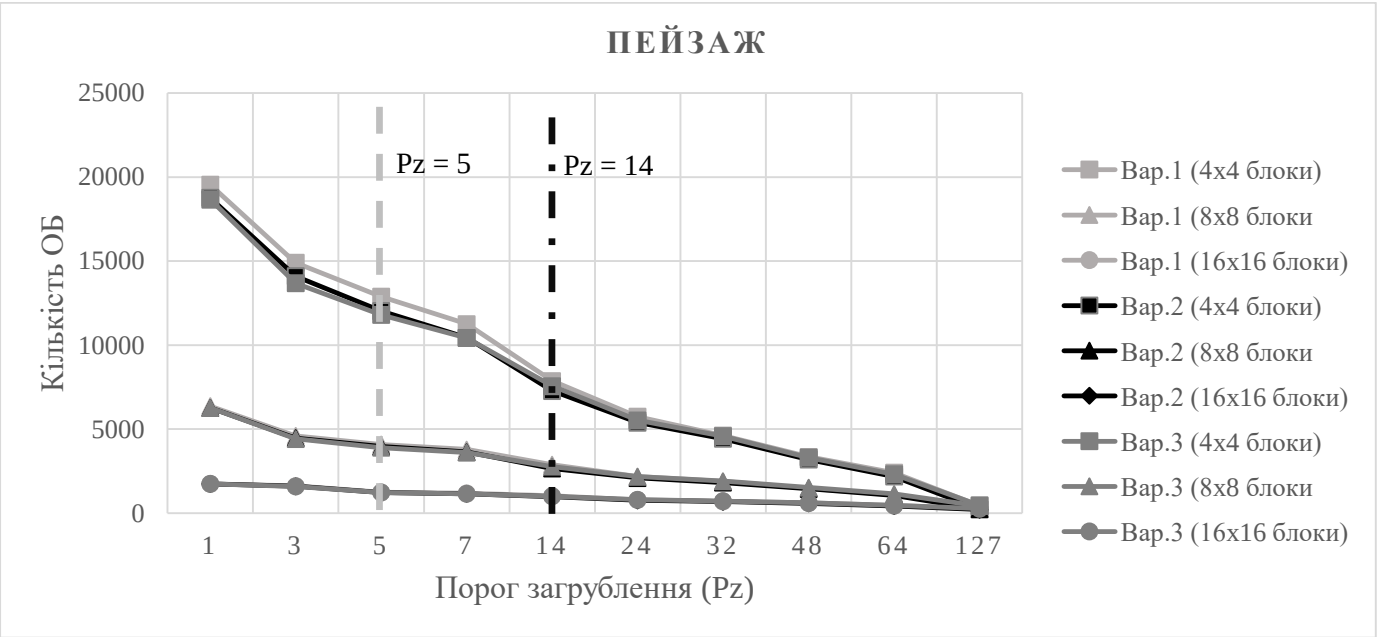


Рисунок 4.4 – Кількість ОБ при різних варіантах передобробки для зображення типу «*Пейзаж*»

Збільшення розмірності ОБ для всіх типів зображень призводить до зменшення загальної кількості серій у мультиплексі 1-го рівня, що звужує базу можливих перестановок (комбінаторику) і таким чином, обмежує захисний потенціал відповідного елемента в структурі ключа екстрактора даних. При цьому, ОБ з більшою розмірністю (наприклад, 16×16 ел, рис. 4.3 - 4.4), значно меншою мірою схильні тенденції до зменшення числа формованих серій (що не є добре з точки зору забезпечення диспаритету кількості блоків контейнера і контенту), ніж при використанні блоків малої розмірності. Результати спроб нелегітимного вилучення даних контенту представлені на рис. 4.5 (*а-д*), 4.6 (*а-д*), що характерні для використання короткого та довгого стека вибірки мультиплексованих параметрів.

Слід зазначити, що в даному циклі експериментів проводилося одночасне мультиплексування відразу обох параметрів (самого ОБ та довжини) базового масиву серій ОБ, як для широкого, так і для короткого стеків вибірки серій (див. Рис. 3.4, 3.8).

Крім того, головною відмінністю представлених на рис. 4.5, 4.6 результатів є, «груба реалізація» процедури передобробки (згладжування) вихідних даних.

У контексті даного матеріалу, під терміном «*груба реалізація*» процедури згладжування, слід розуміти навмисне використання завищених значень порога помітності спотворень «P_z», причому одразу на двох етапах роботи алгоритму [1]: етап передобробки (згладжування) вхідних даних та етап формування масиву серій ОБ.

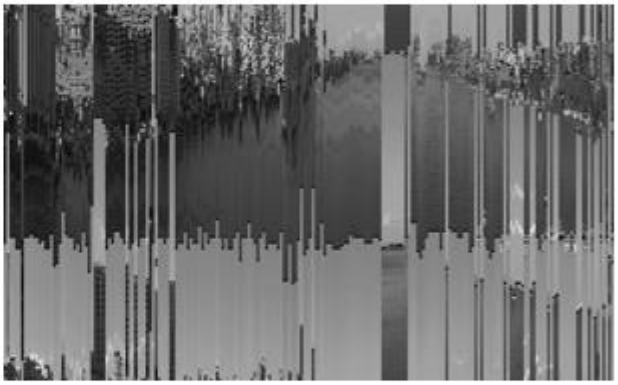
Використання критичних параметрів обробки вихідних даних виключає розумний компроміс між статистичними особливостями тестових зображень (див. Рис. 4.5(е), 4.6(е)) та особливостями зорової системи людини [19,20].

Однак, використання навмисно завищених значень «P_z», послідовно на 2-х етапах обробки, дозволяє проявити основні ефекти, що виявляються внаслідок використання критичних параметрів налаштувань досліджуваного прототипу стеганоалгоритму, з одного боку, і відобразити динаміку зміни характерних артефактів (наслідком використання механізму міжблочного мультиплексування). поточних параметрів масиву довжин серій ОБ), з іншого боку.

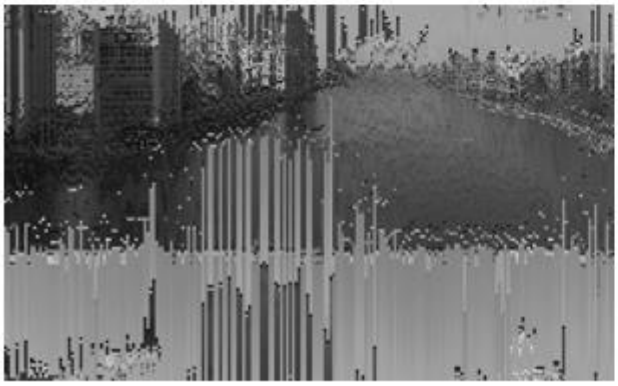
а) Короткий стек (Pz = 14);

б) Короткий стек (Pz = 24);

в) Короткий стек (Pz = 48);



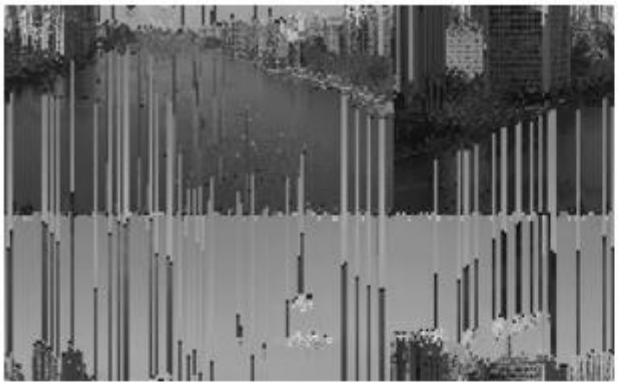
г) Короткий стек (Pz = 64);



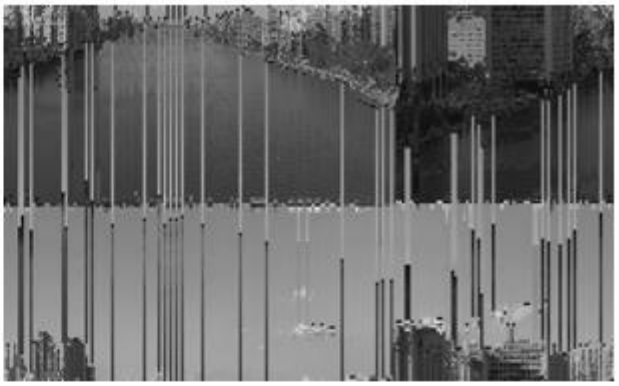
д) Короткий стек (Pz = 7);

е) Вихідне зображення

Рисунок 4.5 – Результати атаки *(а-д)* зображення *(е)* для ***короткого*** стеку на 1-му рівні мультиплексування при різних *Pz*
(пейзаж; 1-й Вар. згладжування; розгортка «стовбці»; ОБ 4×4 ел.)



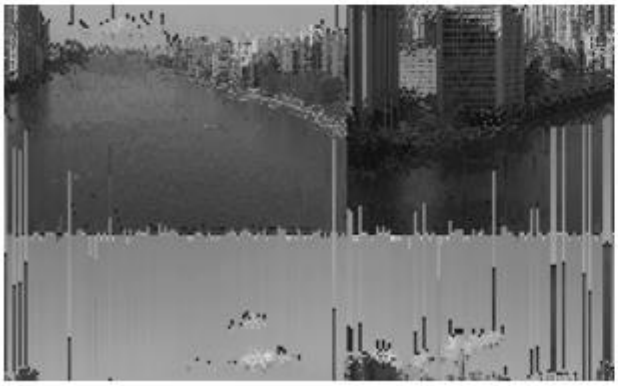
а) Довгий стек (Pz = 14);



б) Довгий стек (Pz = 24);

в) Довгий стек (Pz = 48);

г) Довгий стек (Pz = 64);



д) Довгий стек (Pz = 7);

е) Вихідне зображення

Рисунок 4.6 – Результати атаки *(а-д)* зображення *(е)* для ***довгого*** стеку на 1-му рівні мультиплексування при різних *Pz*
(пейзаж; 1-й Вар. згладжування; розгортка «стовбці»; ОБ 4×4 ел.)

Важливо підкреслити, що використання різних значень P_z на різних етапах роботи алгоритму дозволяє отримати принципово різні результати. Так, наприклад, використання на етапі згладжування вихідних даних, найбільш прийнятних значень P_z (значення від 1 до 5, див. Рис. 4.3 - 4.4) [20] дозволяє зберегти спочатку високу якість вихідних даних, залишаючи можливості для подальшого коригування поточних параметрів базового масиву серій ОБ (шаг №3 на рис. 3.9), виходячи з міркувань забезпечення необхідного рівня диспропорції кількості блоків контенту та контейнера. Таке коригування, забезпечується за допомогою використання на етапі формування базового масиву серій (шаг №3, рис. 3.9), кілька більших значень P_z, ніж те, яке було використане на етапі згладжування (шаг №2, рис. 3.9).

Як «робочі пари» значень P_z, що дають хороші результати, можна вважати, наприклад, такі співвідношення: 1/3, 2/5, 2/4 (де перше число відповідає значенню P_Z, використовуваному на 1-му кроці, а друге число, на 2-му кроці алгоритму.

Слід мати на увазі, що можлива й інша параметрична модель алгоритму. Наприклад, використання великих значень порогу загрублення P_Z (значення в діапазоні від 15 до 127, див. Рис. 4.3 - 4.4) одразу на етапі попередньої обробки (рис. 4.5 - 4.6 (*а-д*)), значною мірою обмежує всі подальші дії на етапі формування масиву серій ОБ, зумовлюючи появу неприйнятних викривлень в оброблюваному зображенні контенту [10]. Прикладом «грубих» робочих пар значень параметру P_Z, можна розглядати, як несиметричні пари, подібні до 14/24, 24/48, так і симетричні співвідношення, наприклад, 14/14, 48/48 (рис. 4.5 - 4.6 (*а-д*)).

Очевидно, що представлені на рис. 4.5 – 4.6 (*б,в,г*) результати мають не більше ніж лабораторний інтерес, проте дозволяють проявити особливості механізму міжблокового мультиплексування параметрів серій ОБ (крок №4 на рис. 3.9 - 3.10), як інструменту протидії спробам неавторизованого вилучення стеганоконтенту [3].

Так, на рис. 3.4 і 3.8 представлені характерні результати невдалої атаки контенту (*помилка в підборі відразу 2-х параметрів мультиплексування (ОБ та їх довжини) для*

різних способів розгортки серій ОБ) при використанні процедур ТІЛЬКИ 1-го рівня захисту, у випадках широкого і короткого стеків вибірки серій.

Спираючись на отримані результати моделювання [4,10,18] можна зробити наступні висновки:

1) Збільшення довжини стека вибірки серій, що розширює комбінаторику міжблочного мультиплексування для обох параметрів сформованих серій ОБ, що значно більшою мірою руйнує кореляційні зв'язки елементів вихідного масиву серій контенту зображення (див. Рис.3,4, 3.8).

2) Збільшення параметра порога загрублення P_z (і на 2-му, і на 3-му кроках алгоритму, рис. 3.9) понад комфортні межі сприйняття (тобто при $P_z > 5$), призводить до плавного зменшення кількості серій блоків ОБ різного змісту (див. Рис. 4.3, 4.4) при одночасному збільшення їх довжини. Ця тенденція добре простежується зменшенням щільності розміщення дійсних серій по всій площі тестового зображення, що атаковано, зі зростанням значення порога загрублення (P_Z) (*див. порівняння зразків (а) та (г), на рис. 4.5 - 4-6*).

3) ОБ з більшою розмірністю, значно меншою мірою схильні до тенденції до збільшення числа формованих серій (що не є добре з точки зору забезпечення диспаритету кількості блоків контейнера і контенту), ніж при використанні блоків малої розмірності (рис. 4.3, 4.4).

4) Використання значень параметру P_Z за межами візуальної помітності спотворень [20], незалежно від етапу їх реалізації (згладжування та/або формування базового масиву серій ОБ), призводить до значних спотворень вихідних даних (див. рис. 4.1 - 4.2). На етапі формування серій ОБ, «грубі» налаштування P_Z, мають найбільш фатальний характер.

5) На етапі формування серій ОБ, граничним значенням для P_Z, слід вважати $P_z = 14$ (при 256 рівнях яскравості). Подальше збільшення P_Z призводить до серйозної деградації вихідних даних (від 15 до 127, див. Рис. 4.3, 4.4).

6) Мультиплексування обох діючих параметрів серій (ОБ та довжини їх серії) вже на малій довжині стека їх вибірки [7,8], дає необхідні результати, що добре підтверджується значною дефрагментацією тестових зображень, представлених на рис. 4.5 - 4.6 (*а-д*).

7) Використані налаштування алгоритму (24/24, 48/48 і 64/64) та представлені для них результати атаки (див. Рис. 4.5 - 4.6 (*б,в,г*)), слід розглядати виключно як демонстратор наслідків «критичних» налаштувань, при реалізації 1-го рівня мультиплексування параметрів серій [7,8,11]. Застосування критичних параметрів обробки вихідних даних, забезпечує хорошу наочність суті процесів, що відбуваються [10].

8) Використання різних способів організації розгортки серій ОБ (див. Рис. 3.4, 3.8) [7], як окремого елемента у загальній структурі складового ключа екстрактора даних, посилює стійкість стеганоконтента до спроб його неавторизованого вилучення.

9) Будь-які маніпуляції з параметром довжини серій на 1-му рівні мультиплексування даних [7,8], створюють хороші умови, у тому числі, для забезпечення легітимації процедури потокового вилучення відеоконтенту з інтегрованою стеганоміткою.

4.2 Результати моделювання процедур дворівневого мультиплексу контенту

Як уже було зазначено раніше (Розділ 2), на момент виконання моделювання до загальної структури складового ключа екстрактора даних входять 6 основних елементів, з них: - 4 активні (тобто ті, зміна стану яких моделювалася), та 2 відключені (зміна їх станів не моделювалася). Слід підкреслити, що під час обробки даних контенту та контейнера частково використовується, також 5 елемент ключа екстрактора, який імітував тільки один стан з двох можливих, тобто встановлював режим симетричної обробки вхідних даних [1].

У табл. 4.1 наведено використовуваний набір настроювальних параметрів (комбінації елементів ключа екстрактора), які визначають параметри обробки даних

на кожному з передбачених етапів обробки даних для демонстрації результатів багаторівневого мультиплексування даних для діючої версії алгоритму.

Таблиця 4.1 – Основні параметри налаштувань алгоритму

Позиція ключа	**Зміст процедур**	**Набір настроювальних параметрів**
1	Розмірність ОБ для зображення-контейнера (розмірність NxN блоків)	4-8-16
2	Діючий спосіб організації розгортки серій ОБ (1 - по стовпчикам; 2- по рядках; 3- «змійка»)	1-2-3
3	Маска перестановок діючих параметрів серій ОБ на **1-му рівні** мультиплексування (1 – Короткий стек, 2- Довгий стек)	1-2
4	Маски перестановок діючих значень (0; 0) для всіх ОБ, на **2-му рівні** мультиплексування (1 – Короткий стек, 2- Довгий стек)	1-2
5	Визначення ознаки симетрії обробки даних контенту та контейнера	Симетричний режим (*за замовчуванням*)
		Несиметричний режим (відключено, не моделювався)

Таким чином поточна версія дослідного алгоритму забезпечує достатній набір основних станів ключових параметрів, які потрібні для моделювання процедур дворівневого мультиплексування даних.

Перший параметр (позиція ключа №1) відповідає за поділ вихідного зображення контенту на блоки розміром N×N пікселів. В процесі моделювання оптимальною розмірністю блоків є розмірність 4×4 (4) 8×8 (8) та 16×16 (16) елементів.

Другий параметр (позиція ключа №2) відповідає за організацію розгортки серій ОБ після розбиття зображення на блоки, в якості демонстратора, доступні три варіанти розгортки, а саме обхід по стовпчикам (1), обхід по рядках (2) та обхід «змійка» (3) [7].

Третій та четвертий параметр (позиція ключа №3 та №4) відповідають за вибір маски перестановок для діючих параметрів серій на 1-му міжблочному

(*використовується маска перестановок діючих параметрів серій ОБ: Короткий стек (1) та Довгий стек (2)*), та 2-му внутриблочному (*використовується маска перестановок для всіх діючих значень (0; 0): Короткий стек (1) та Довгий стек (2)*) рівні мультиплексування даних.

У табл. 4.2 наведено набір використовуваних настроювальних параметрів (комбінацій ключа екстрактора), які визначають свою позицію в загальній структурі ключа екстрактора даних, при реалізації процедур багаторівневого мультиплексу вхідних даних та відображають загальну концепцію гібридного стеганоалгоритму, в його діючої версії [1,7].

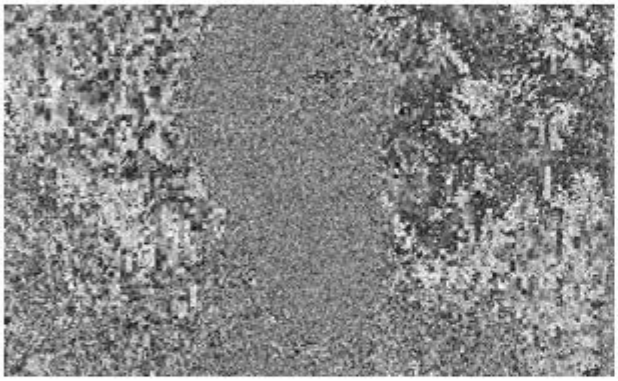
Результати моделювання процедур дворівневого мультиплексу даних, для різних комбінацій ключа екстрактора, представлені на рис. 4.7 – 4.11, де на рис. 4.7 – 4.11 (*в-е*) представлені «дельти» (тобто різниця між вихідним та атакованим зображеннями): - *max* помилка відповідає білому коліру (тобто яскравість «255»), а *min* помилка (повний збіг) - це чорний колір (яскравість «0»).

Таблиця 4.2 – Комбінації ключа екстрактора

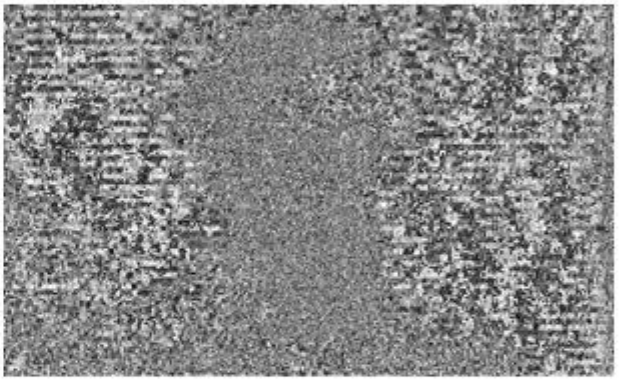
Комбінації ключа екстрактора											
Позиція ключа	**P_z = 3**					**P_z = 14**					**Набір настроювальних параметрів**
	Комбінації										
	1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	
1	*8*	*8*	*8*	*8*	*16*	*8*	*8*	*8*	*8*	*16*	**4-8-16**
2	*1*	*3*	*3*	*3*	*3*	*1*	*3*	*3*	*3*	*3*	**1-2-3**
3	*1*	*1*	*2*	*2*	*2*	*1*	*1*	*2*	*2*	*2*	**1-2**
4	*1*	*1*	*1*	*2*	*2*	*1*	*1*	*1*	*2*	*2*	**1-2**
5	-	-	-	-	-	-	-	-	-	-	**Симетричний режим (за замовчуванням)**

а) Комбінація ключа екстрактора №1 (СКП = 42.874, PSNR = 31.809, P_z = 3);

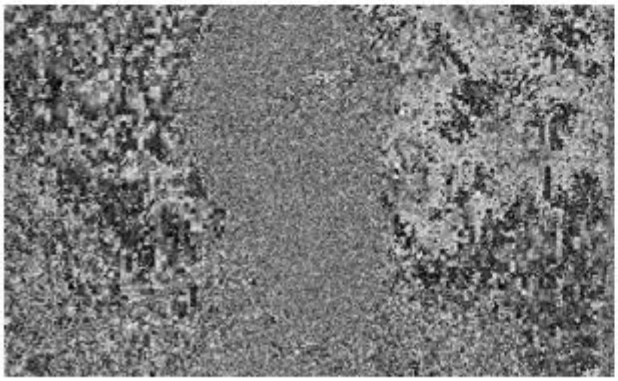
б) Комбінація ключа екстрактора №2 (СКП = 41.803, PSNR = 31.919, P_z = 3);



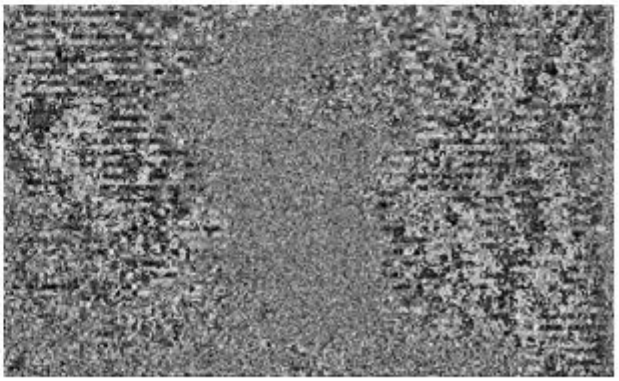
в) Комбінація ключа екстрактора №1 (Інверсія);



г) Комбінація ключа екстрактора №2 (Інверсія);

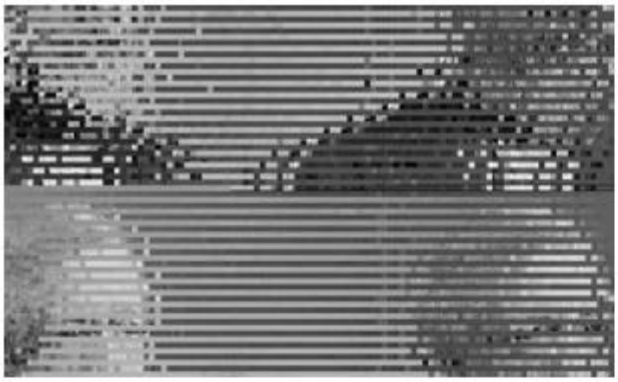


д) Комбінація ключа екстрактора №1 (Негатив);

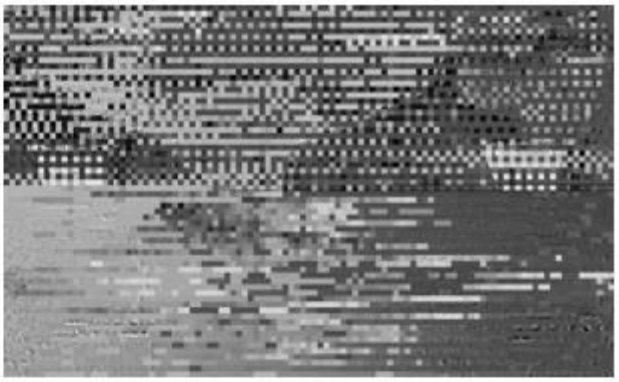


е) Комбінація ключа екстрактора №2 (Негатив);

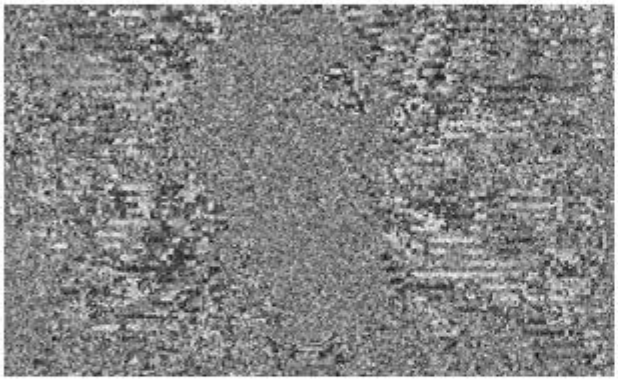
Рисунок 4.7 – Результати моделювання процедур дворівневого мультиплексу даних для комбінацій №№ 1 і 2, ключа екстрактора



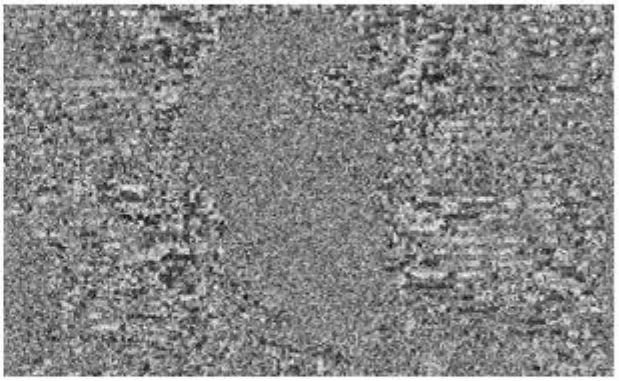
а) Комбінація ключа екстрактора №3 (СКП = 67.187, PSNR = 29.858, Pz = 3);



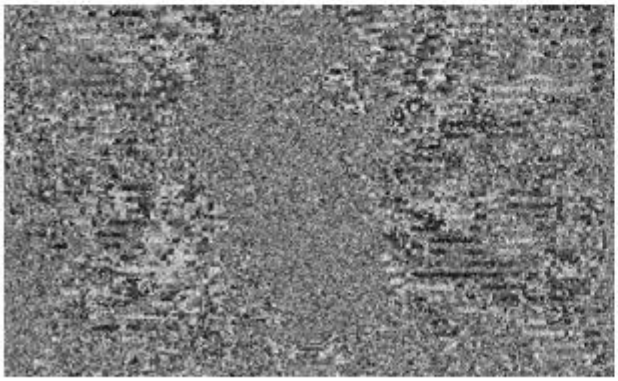
б) Комбінація ключа екстрактора №4 (СКП = 64.804, PSNR = 30.015, Pz = 3);



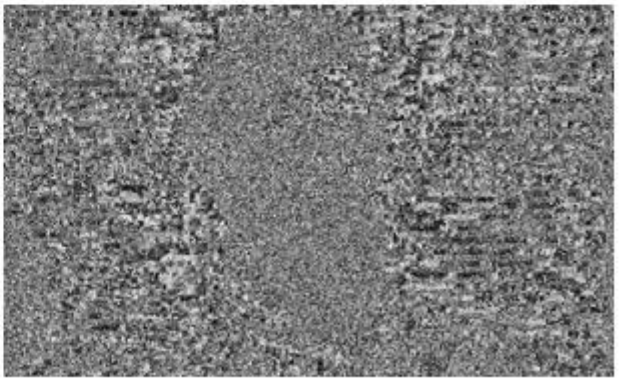
в) Комбінація ключа екстрактора №3 (Інверсія);



г) Комбінація ключа екстрактора №4 (Інверсія);

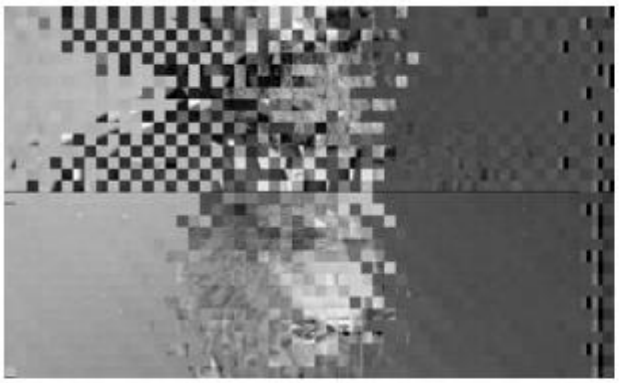


д) Комбінація ключа екстрактора №3 (Негатив);



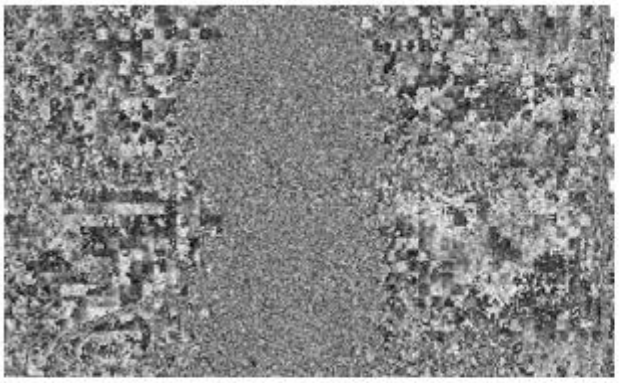
е) Комбінація ключа екстрактора №4 (Негатив);

Рисунок 4.8 – Результати моделювання процедур дворівневого мультиплексу даних для комбінацій №№ 3 і 4, ключа екстрактора

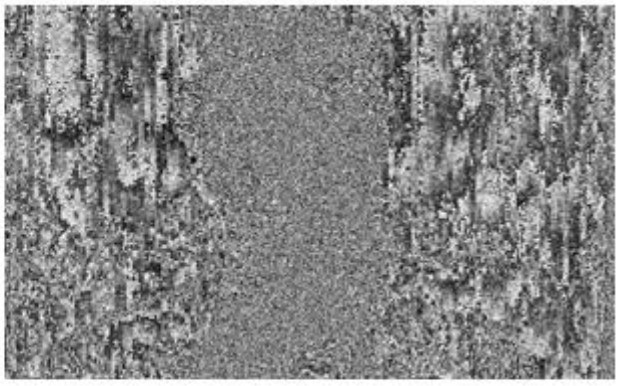


а) Комбінація ключа екстрактора №5 (СКП = 53.759, PSNR = 30.82б, P_z = 3);

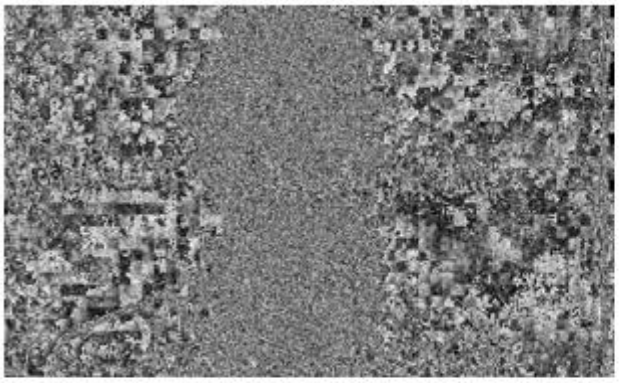
б) Комбінація ключа екстрактора №1 (СКП = 55.265, PSNR = 30.70б, P_z = 14);



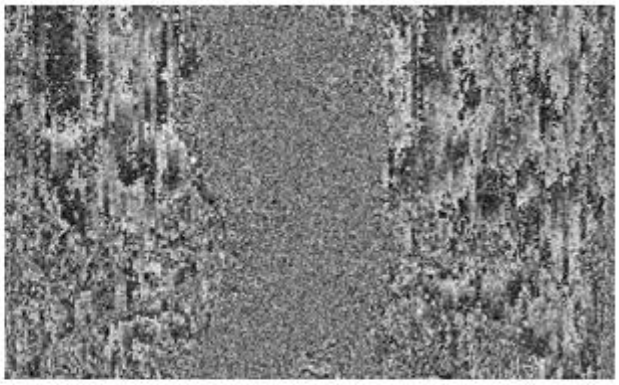
в) Комбінація ключа екстрактора №5 (Інверсія);



г) Комбінація ключа екстрактора №1 (Інверсія);

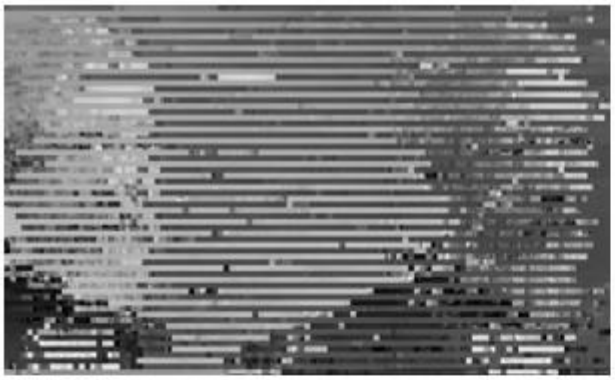


д) Комбінація ключа екстрактора №5 (Негатив);

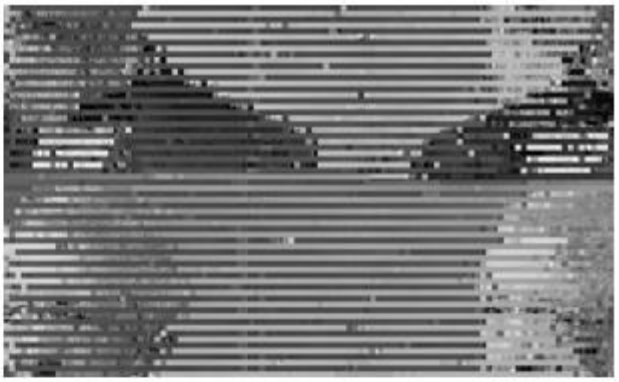


е) Комбінація ключа екстрактора №1 (Негатив);

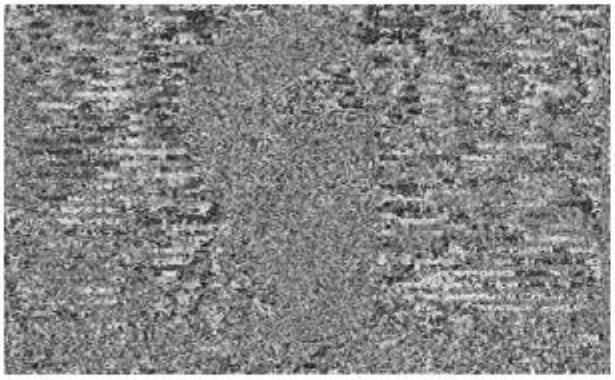
Рисунок 4.9 – Результати моделювання процедур дворівневого мультиплексу даних для комбінацій №№ 5 і 1, ключа екстрактора



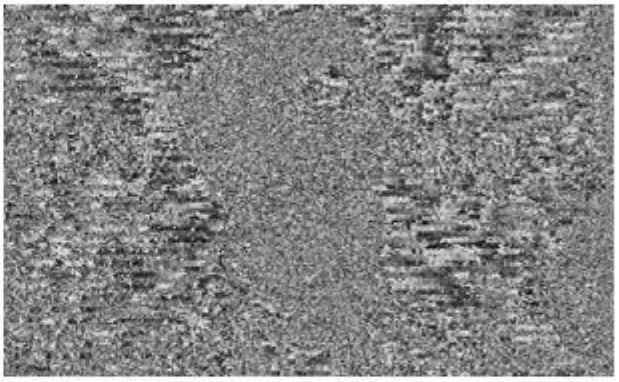
а) Комбінація ключа екстрактора №2 (СКП = 62.829, PSNR = 30.149, P_z = 14);



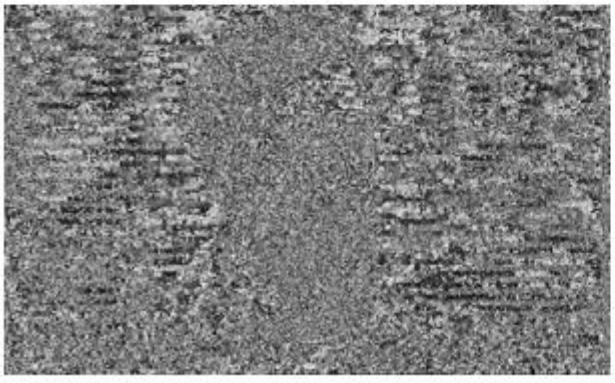
б) Комбінація ключа екстрактора №3 (СКП = 73.793, PSNR = 29.451, P_z = 14);



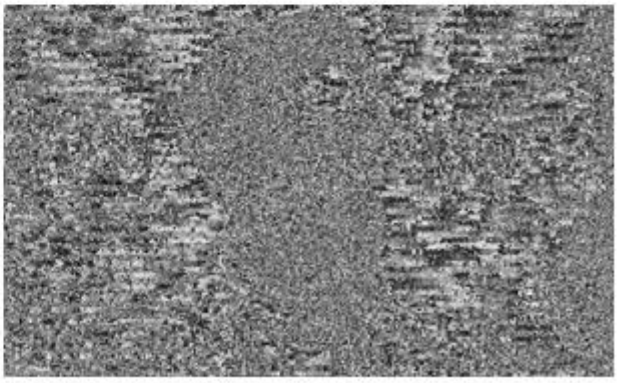
в) Комбінація ключа екстрактора №2 (Інверсія);



г) Комбінація ключа екстрактора №3 (Інверсія);



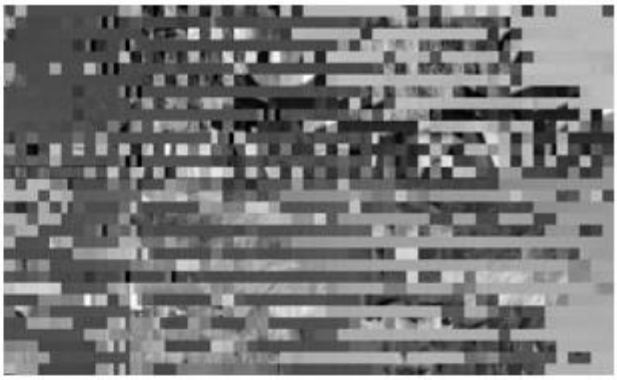
д) Комбінація ключа екстрактора №2 (Негатив);



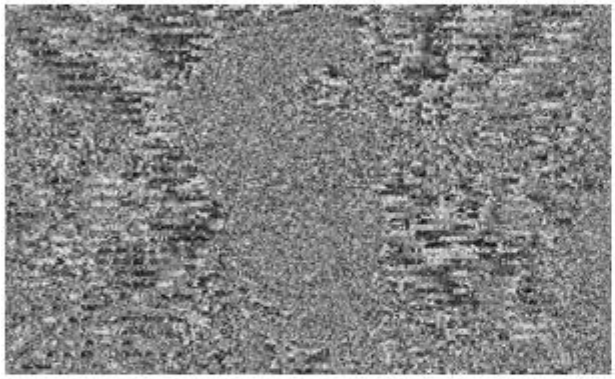
е) Комбінація ключа екстрактора №3 (Негатив);

Рисунок 4.10 – Результати моделювання процедур дворівневого мультиплексу даних для комбінацій №№ 2 і 3, ключа екстрактора

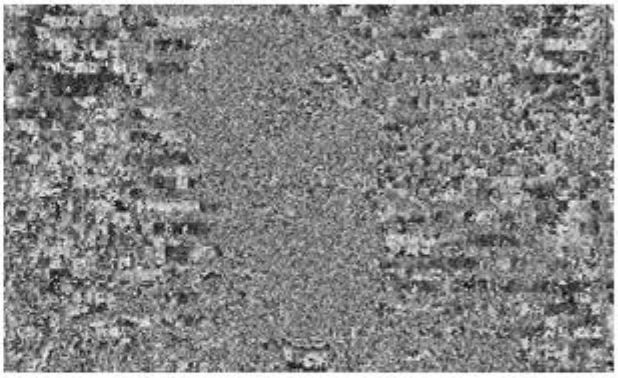
а) Комбінація ключа екстрактора №4 (СКП = 74.591, PSNR = 29.404, P_z = 14);



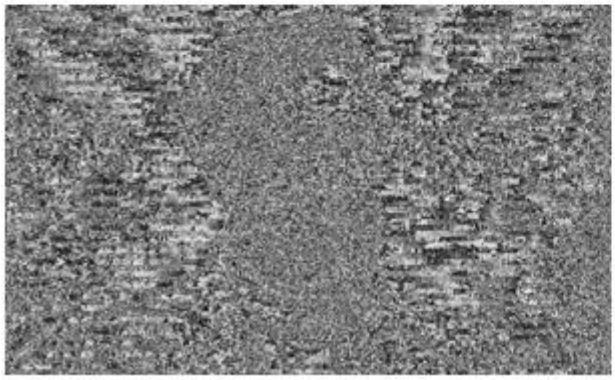
б) Комбінація ключа екстрактора №5 (СКП = 79.149, PSNR = 29.146, P_z = 14);



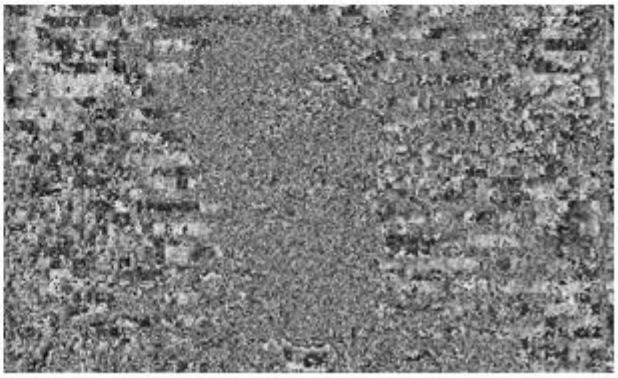
в) Комбінація ключа екстрактора №4 (Інверсія);



г) Комбінація ключа екстрактора №5 (Інверсія);

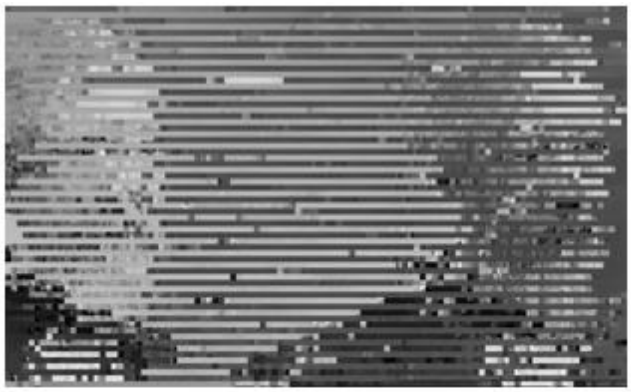


д) Комбінація ключа екстрактора №4 (Негатив);



е) Комбінація ключа екстрактора №5 (Негатив);

Рисунок 4.11 – Результати моделювання процедур дворівневого мультиплексу даних при комбінацій №№ 4 і 5, ключа екстрактора



а) Короткий стек
(СКП = 62.829, PSNR = 30.149, P_z = 14);

б) Довгий стек
(СКП = 74.591, PSNR = 29.404, P_z = 14);

Рисунок 4.12 – Результати моделювання дворівневого мультиплексу даних для ключових комбінацій №№ 2 та 4 (*короткий і довгий стеки, Табл. 4.2)*

З отриманих результатів, наочно видно, що при використанні різних комбінацій ключових параметрів, можна отримати дуже різні результати, які роблять значний внесок у загальний ефект. Отримані результати підтверджують, що хибний підбор використаних параметрів обробки контенту, істотно ускладнює його неавторизовану екстракцію. Ця теза підтверджується суттєвим руйнуванням тестових зображень, на прикладі комбінацій ключа екстрактора №1-2 (табл. 4.2) для двох випадків (P_z = 3 та P_z = 14) при довжині стеку, навіть у 4 серії ОБ [15].

З цієї причини на наведених тестових зразках добре проглядається періодичність артефактів злому (наприклад, подвоєння обличчя і пропорційний зсув окремих фрагментів, що обумовлено малої базою переміщуваних параметрів).

Іншими словами, використання більш складних комбінацій ключа екстрактора, наприклад комбінації ключа №5 (P_z = 3 та P_z = 14), дозволяє відчутно зруйнувати вихідний контент та внести серйозні труднощі, щодо процесу його ідентифікації.

На рис. 4.13, 4.14 представлено графіки зміни значень СКП та PSNR, залежно від використаної ключової комбінації №1 – №5 для 3-х різних типів зображень, що підтверджує необхідність правильного підходу до вибору діючих ключових параметрів, щоб забезпечити хороші умови для легітимації процедур вилучення стеганоконтента з контейнера.

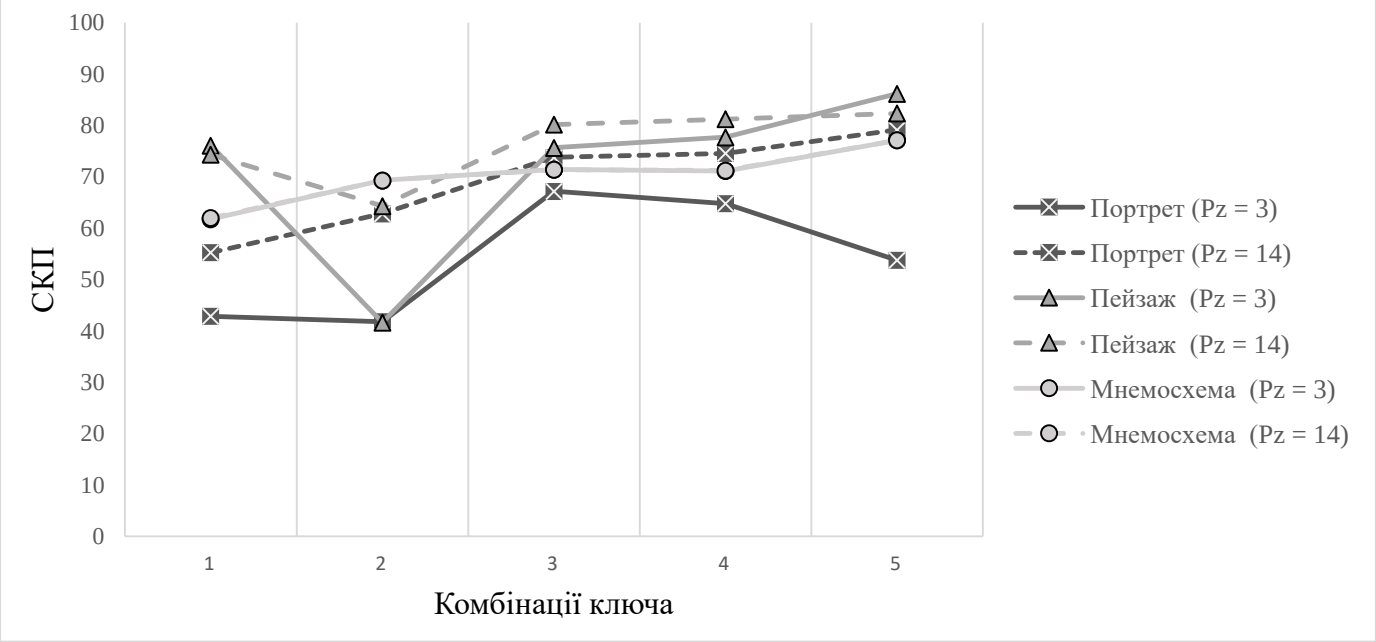


Рисунок 4.13 –Значення СКП для різних ключових комбінацій
(*для 3-х різних типів зображень*)

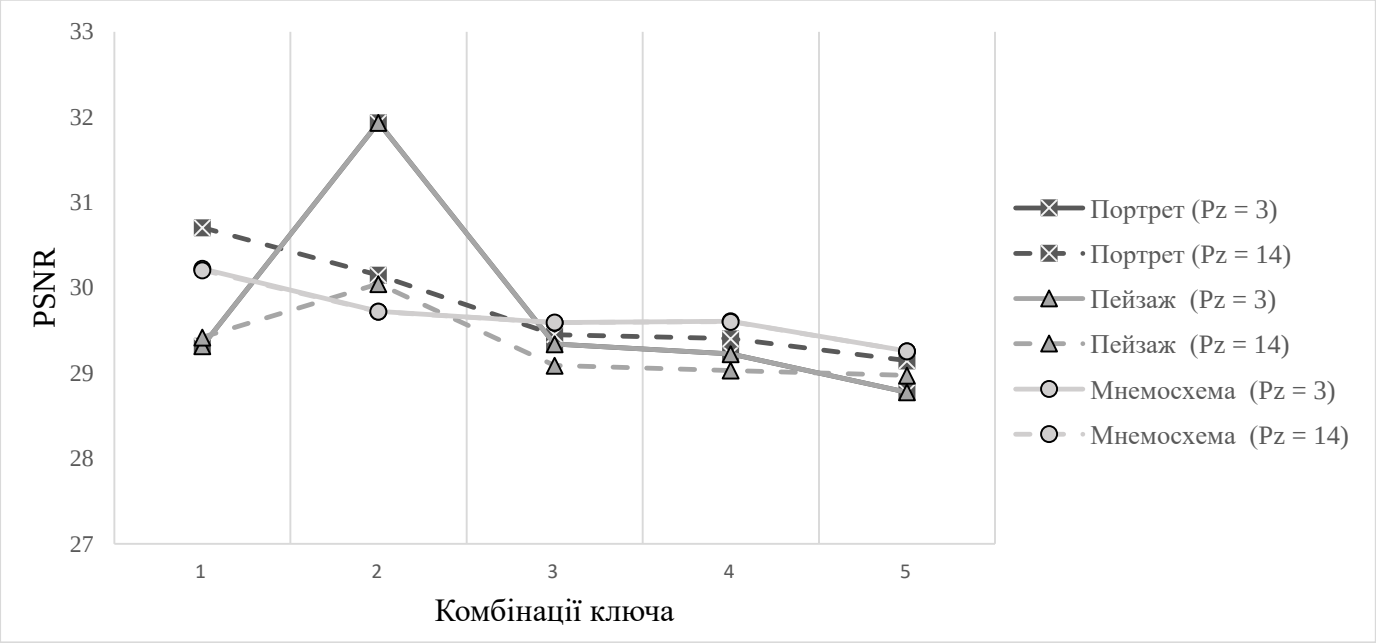


Рисунок 4.14 –Значення PSNR для різних комбінацій ключа екстрактора
(для 3-х різних типів зображень)

Як зазначалось раніше, в рамках даної роботи була використана «Лайт» версія тестового алгоритму, яка обмежена мультиплексуванням поточних параметрів контенту, тільки на 2-х процедурних рівнях [15]:

1) міжблоковий рівень (ОБ та параметри довжин їх серій);

2) внутрішньоблоковий рівень (параметри середньої яскравості ОБ).

При формуванні 1-го та 2-го рівня мультиплексу необхідно застосовувати більш складний алгоритм для генерації випадкових чисел (тобто маски перемішування) для якісного перемішування (перестановок) даних на 2-х рівнях обробки, що наочно підтверджується при порівнянні результатів злому тестового зображення при використані короткого та довгого стеків вибірки діючих параметрів мультиплексування (див. Рис. 3.11 та 4.12).

Слід підкреслити, про необхідність використання на 2-му етапі більш складних способів розгортки серій та вибору з них окремих параметрів. Тому, хорошим варіантом розгортки серій є способи (зиґзаґ або спіраль (у будь-якому вигляді)), оскільки більшою мірою руйнують вихідні кореляційні зв'язки між сусідніми серіями ОБ та забезпечать одночасне переміщення між стовпцями та рядками вихідного кадру та забезпечуючи хороші умови протидії алгоритму до зламування цього елемента у складі ключа екстрактора.

Для додаткового захисту можна застосувати також принцип «кратності» проходів під час вибірки поточних параметрів масиву серій, тобто на першому проході застосовується розгортка серій ОБ, наприклад, «зиґзаґ». При першому проході «працюємо» з кожним парним блоком зображень - формуючи з них свій умовний «напівстек - А» ОБ, а на другому проході переглядаємо неторкнуті непарні блоки, формуючи з них другий «напівстек - Б» серій ОБ.

Причому в обох проходах правило роботи з самими серіями (порівняння на їхню подобу або ідентичність змісту) залишається таким самим, як було і у випадку даної роботи, тобто з одним загальним масивом.

Таким чином атакуючий неминуче зіткнеться з серйозною проблемою, щоб зуміти співвіднести параметри одразу двох вибірок (напівстеків ОБ) в рамках ще невідомого для нього способу реалізації самої розгортки.

Використання спеціальних процедур передобробки даних дозволяє забезпечити необхідний диспаритет початкових умов (властивість об'єктів) для подальшої реалізації стегановставки при зниженні загальної обчислювальної складності всього алгоритму, а вибрана концепція реалізації запропонованого конструктиву алгоритму, в разі його доробки, дозволить позиціонувати його, як автономне рішення для забезпечення захисту даних у складі мобільних платформ.

За результатами моделювання, гібридний алгоритм, підтвердив свої простоту та невимогливість до потрібних ресурсів (див. Рис. 1.6 та Рис. 12 в [2]).

Перспективою на майбутнє є удосконалення окремих процедур обробки даних в 3-х основних напрямах:

– забезпечення принципу «кратності» проходів під час вибірки поточних параметрів масиву серій в межах обраного способу розгортки;

– забезпечення режиму несиметричною обробки блоків контенту та контейнера на перших 2-х етапах обробки (*тобто, згладжування і формування серій ОБ*);

– забезпечення режиму обробки несиметричних блоків контенту, наприклад ОБ з розмірністю 4×8, 6×12, 8×16 елементів тощо [6];

– забезпечення функцій інкапсуляції (стегановставки) контенту на 3-му рівні мультиплексу вхідних даних (елемент № 6 в табл. 2.1) [17];

– активація ключового елементу на рівні 6+ (див. Табл. 2.1), що посилює загальну стійкість ключа (рис. 2.1) до підбору діючих параметрів стегановставки;

– вдосконалення (ускладнення) діючих способів розгортки серій ОБ.

4.3 Моделювання атаки контенту в разі компрометації відразу 2-х рівнів мультиплексування

Результати спроби злому (зображень 2-х типів) контенту за умов успішного підбору діючих параметрів кодування одразу для двох рівнів обробки, представлено на рис. 4.15 - 4.16.

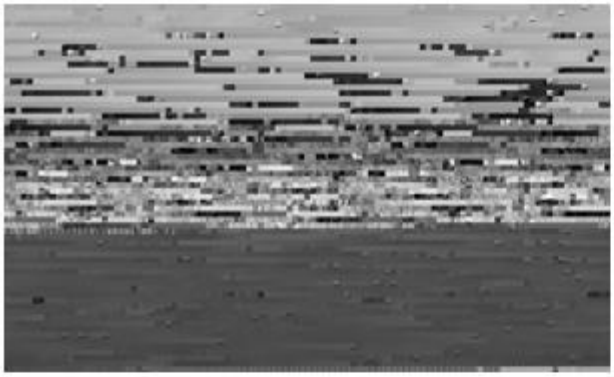
В даному випадку моделювалася ситуація при якій атакуючий припустився помилки у визначенні діючого способу розгорнення серій ОБ (див. рис. 3.1), тобто зламано 2 із 3-х параметрів обробки (позиції №№3-4 у табл. 2.1). Вихідний та використаний атакуючим, способи організації розгортки серій ОБ, представлені відповідними парами станів (наприклад, *кодування «стовпчики» -> злом «рядки»),* які вказані під кожною мініатюрою.

Як випливає з рис. 4.15 - 4.16, незалежно від діючих варіантів обробки даних-контенту на будь-якому з двох рівнів мультиплексування (рис. 3.9), помилка у діючому способі організації розгорнення масиву серій ОБ, носить фатальний характер, і не дозволяє ідентифікувати контент.

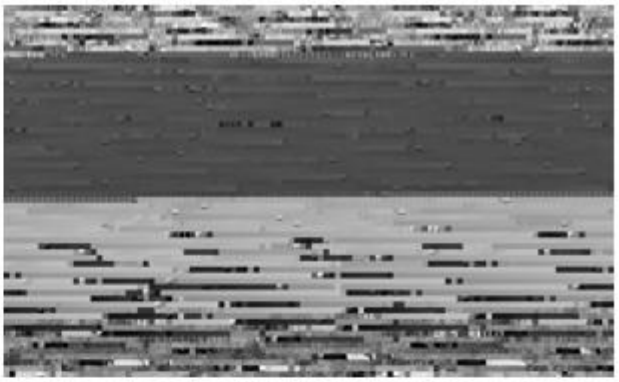
Таким чином, важливість ключової позиції, що характеризує діючий спосіб розгорнення серій, складно переоцінити. Враховуючи легковажність реалізації цієї процедури та потенційне різноманіття варіантів її реалізації, можна стверджувати, що відповідний елемент у структурі складового ключа екстрактора, за своєю значимістю, не поступається обом процедурним рівням обробки.

Крім того, використання, навіть одного параметра розгортки серій (без ключових позицій № 3-4, в табл. 2.1), при необхідності, може забезпечити «полегшений» режим стегановставки (*наприклад, за умови обмеженого заряду вбудованої батареї гаджета, що використовується*).

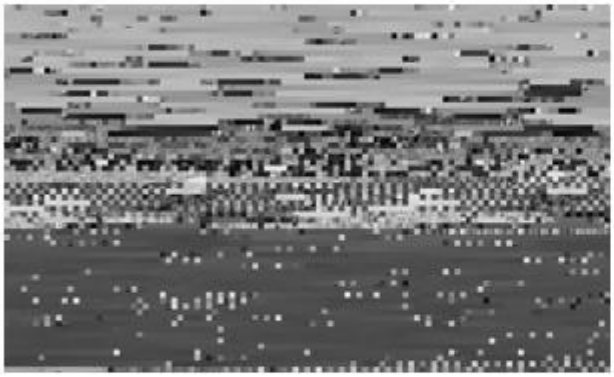
Загалом, використання такого режиму інкапсуляції, в сукупності з рекомендованими розмірностями ОБ, є гідною альтернативою, в умовах жорсткого енергодефіциту базового пристрою.



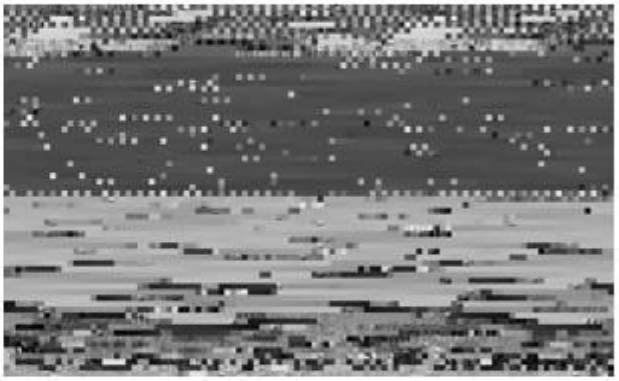
а) Level 1 (Коротк.Стек) / Level 2 (Коротк.Стек) (кодування «стовпчики» -> злом «рядки»);



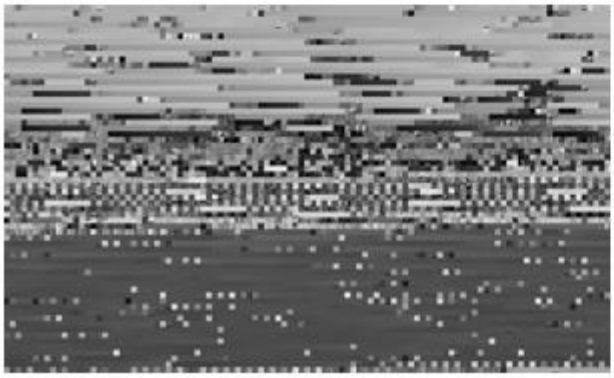
б) Level 1 (Довг.Стек) / Level 2 (Коротк.Стек) (кодування «стовпчики» -> злом «рядки»);



в) Level 1 (Коротк.Стек) / Level 2 (Довг.Стек) (кодування «стовпчики» -> злом «змійка»);



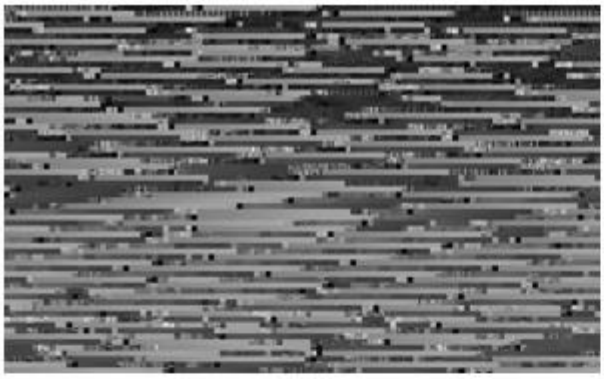
г) Level 1 (Довг.Стек) / Level 2 (Довг.Стек) (кодування «стовпчики» -> злом «змійка»);



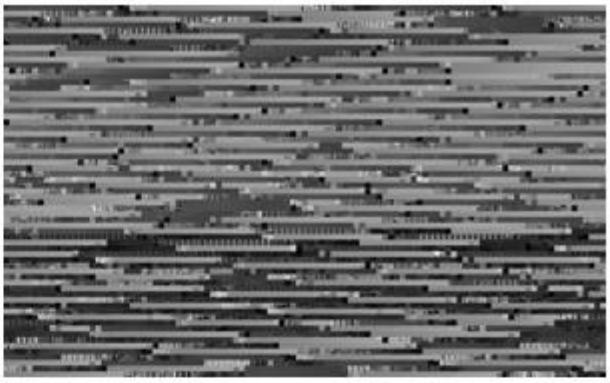
д) Level 1 (Коротк.Стек) / Level 2 (Довг.Стек) (кодування «стовпчики» -> злом «рядки»);

е) вихідне зображення типу «портрет»;

Рисунок 4.15 – Результати **хибного** підбору параметру *«розгортка серій»* при вдалому підборі (*зломі*) обох рівнів мультиплексування контенту *(для P_z =14; ОБ 8×8 ел.)*



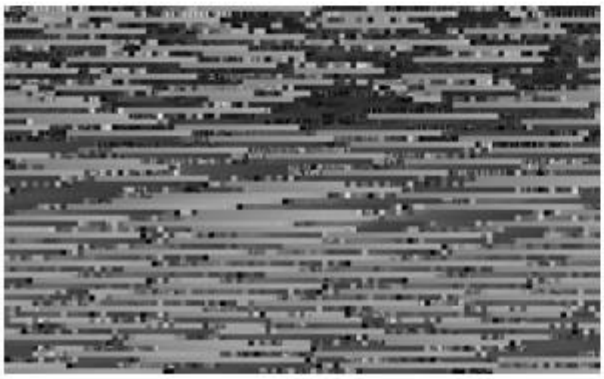
а) Level 1 (Коротк.Стек) / Level 2 (Коротк.Стек) (кодування «стовпчики» -> злом «рядки»);



б) Level 1 (Довг.Стек) / Level 2 (Коротк.Стек) (кодування «стовпчики» -> злом «рядки»);

в) Level 1 (Коротк.Стек) / Level 2 (Довг.Стек) (кодування «стовпчики» -> злом «змійка»);

г) Level 1 (Довг.Стек) / Level 2 (Довг.Стек) (кодування «стовпчики» -> злом «змійка»);



д) Level 1 (Коротк.Стек) / Level 2 (Довг.Стек) (кодування «стовпчики» -> злом «рядки»);

е) вихідне зображення типу «пейзаж»;

Рисунок 4.16 – Результати **хибного** підбору параметру *«розгортка серій»* при вдалому підборі (*зломі*) обох рівнів мультиплексування контенту *(для P_z =14; ОБ 8×8 ел.)*

ВИСНОВКИ

1) Застосування для обробки контейнера та контенту різних варіантів предобробки та/або різних установчих параметрів алгоритму, сприяє створенню необхідних стартових умов для покращення характеристик формування серій ОБ та дозволяє поліпшити комбінаторику мультиплексу серій. При цьому, кількість серій ОБ залежить від типу зображення, розмірності ОБ та параметрів згладжування.

2) Збільшення розмірності ОБ вихідних зображень, помітно зменшує загальну кількості формованих серій ОБ, незалежно від реалізованих варіантів попередньої обробки вихідних даних, та декілька нівелює процес зменшення обчислювальної складності всього алгоритму (внаслідок збільшення загальної чисельності ОБ, що потребують проведення кодування з перетворенням).

3) Для всіх варіантів передобробки реалістичних зображень, збільшення порога загрублення яскравості сусідніх елементів, більш ніж на 15 градацій (у більшості випадків, це фактично верхня межа порога візуальної помітності спотворень), не призводить до подальшого збільшення довжини серій, ідентичних за вмістом блоків зображень.

4) Використання значень параметру P_Z за межами візуальної помітності спотворень [20], незалежно від етапу їх реалізації (згладжування та/або формування базового масиву серій ОБ), призводить до значних спотворень вихідних даних (див. Рис. 4.1 - 4.2). На етапі формування серій ОБ, «грубі» налаштування P_Z, мають найбільш фатальний характер.

5) Варіюючи розмірністю маски згладжування і типом контейнера можна забезпечити необхідний компроміс, між допустимим ступенем спотворень контейнера і кількістю ОБ, що забезпечує необхідну комбінаторику використовуваних рівнів мультиплексу даних, де кожен з рівнів визначає свою позицію в структурі складового ключа екстрактора даних.

6) Використання спеціальних процедур передобробки даних [4,6] дозволяє забезпечити необхідний диспаритет початкових умов для подальшої реалізації стегановставки при зниженні загальної обчислювальної складності всього алгоритму. Реалізована концепція конструктиву алгоритму [1], дозволяє позиціонувати його, як автономне малоресурсне програмне рішення для забезпечення захисту даних у складі різних мобільних платформ. При певному доопрацюванні можлива розподілена реалізація алгоритму (сервер - клієнт).

7) Використання принципу кодування довжин серій при реалізації процедур міжблочного мультиплексу даних створює хорошу основу для протидії спробам несанкціонованого доступу к контенту, зменшує обчислювальну складність всього алгоритму (за рахунок скорочення загальної кількості ОБ) та створює необхідні вихідні умови для реалізації процедур міжблочного мультиплексу даних.

8) Використання параметра «довжин серій» ОБ, як один з елементів складеного ключа екстрактора даних, дозволяє отримати набагато більш суттєвіший ефект, ніж при реалізації перестановок тільки за допомогою ОБ, оскільки параметр довжин серій значно більшою мірою руйнує кореляційні зв'язки елементів вихідного масиву серій контенту зображення (див. Рис. 3,4, 3.8).

9) Опорні блоки та параметри їх довжин серій є основними процедурними елементами на етапі міжблокової обробки контенту (див. Рис. 3.9, крок №4);

10) Розмірність ОБ та різні способи організації розгортки серій (рис. 3.9 - 3.10) визначають порядок реалізації процедур міжблокової обробки даних і формують відповідні позиції в структурі складеного ключа екстрактора (див. Табл. 2.1);

11) Діючий спосіб розгортки серій, опосередковано визначає структуру артефактів атакованого тестового зображення за умови вдалого підбору одного з діючих механізмів (рис.3.9) мультиплексування (див. Рис. 3.11 - 3.12);

12) Для ускладнення роботи стеганоаналітика необхідно використовувати більш складніші варіанти організації розгортки серій (наприклад, зиґзаґ або спіраль). При цьому, внесення навіть невеликих змін до принципу організації розгортки серій,

наприклад, перехід від розгортки по рядках до варіанта «змійка», вносить істотні зміни до змісту контенту, що відтворюється (рис. 3.11-3.12 (*в-г*) проти (*д-е*)).

13) Мультиплексування обох діючих параметрів серій (ОБ та довжини їх серії) вже на малій довжині стека їх вибірки [7,8], дає необхідні результати, що добре підтверджується значною дефрагментацією тестових зображень, представлених на рис. 4.5 - 4.6 (*а-д*).

14) Будь-які маніпуляції з параметром довжини серій на 1-му рівні мультиплексування даних [7,8], створюють хороші умови, у тому числі, для забезпечення легітимації процедури потокового вилучення відеоконтенту з інтегрованою стеганоміткою.

15) При використанні різних комбінацій ключа екстрактора, тобто діючих параметрів багаторівневого мультиплексу даних, можна отримати різні результати, які роблять значний внесок у загальний ефект.

16) При формуванні 1-го та 2-го рівня мультиплексу необхідно застосовувати більш складний алгоритм для генерації випадкових чисел (тобто маски перемішування) для якісного перемішування даних на 2-х рівнях обробки, це наочно підтверджується при порівнянні короткого та довгого стека.

17) Кожен із 2-х використаних рівнів мультиплексування (міжблоковий та внутрішньоблоковий), роблять значний внесок у загальний ефект. Навіть вдалий підбір діючої комбінації, у співвідношенні 2 із 3-х (тобто спосіб розгортки + один із двох рівнів мультиплексу), відчутно руйнує вихідний контент (рис. 3.11-3.12).

18) Важливість ключової позиції, що характеризує діючий спосіб розгорнення серій, складно переоцінити. Враховуючи легковажність реалізації цієї процедури та потенційне різноманіття варіантів її реалізації, можна стверджувати, що відповідний елемент у структурі складового ключа екстрактора, за своєю значимістю, не поступається обом процедурним рівням обробки.

19) Збільшення довжини стека вибірки для діючих параметрів мультиплексування, істотно ускладнює неавторизовану екстракцію контенту з

контейнера. Ця теза підтверджується суттєвим руйнуванням тестових зображень, на довжині короткого та довгого стеку (див. Рис. 3.11 – 3.12, 4.7 – 4.11). З цієї причини на наведених тестових зразках добре проглядається періодичність артефактів злому (наприклад, подвоєння обличчя тощо).

Для вирішення питань забезпечення оперативної та малоресурсної стегановставки з необхідними показниками скритності факту інкапсуляції даних та стійкості до спроб нелегітимної екстракції прихованого контенту, змодельований прототип гібридного стеганоалгоритму, демонструє хороші результати при використанні різних властивостей, ефектів та методів кодування відеоданих.

Вибрана концепція алгоритму забезпечує широкий діапазон комбінаторики параметрів кодування (і для контейнера і для контенту), що потенційно розширює варіативність реалізацій набору настроювальних параметрів складового ключа екстрактора даних [1], а отримані результати в ході виконання цієї роботи наглядно підтверджують ці ствердження, що будь-які маніпуляції з параметрами складового ключа екстрактора даних, створюють хороші умови, в тому числі, для легітимації процедури потокового вилучення відеоконтенту з інтегрованою стеганометкою.

Враховуючи «легковажність» подібної обробки даних, цей напрямок представляє інтерес у галузі програмних рішень для мобільних гаджетів, з характерним для них консенсусом протиріч: «ресурсоємність обробки даних – обмеженість джерела енергії».

В якості перспективи на майбутнє слід вважати наступні напрями удосконалення розглянутих процедур:

– забезпечення принципу «кратності» проходів під час вибірки поточних параметрів масиву серій;

– забезпечення режиму несиметричною обробки контенту та контейнера (*різної розмірності блоків зображень*);

– забезпечення функцій інкапсуляції (стегановставки) контенту на 3-му рівні мультиплексу вхідних даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лесная Ю. Е., Гончаров Н. А., Малахов С. В. Отработка концепта многоуровневого мультиплекса данных гибридного стеганоалгоритма. *Current issues of science, prospects and challenges* : матеріали 1-ї міжнар. наук.-техн. конф., 17 груд. 2021 р. м. Сідней, Австралія. т. 2. С. 48 – 56. – URL: https://doi.org/10.36074/scientia-17.12.2021 (дата звернення: 01.11.2022).
2. Гончаров М., Лєсная Ю., Малахов С. Дослідження властивостей прототипу гібридного стеганоалгоритму. *Комп'ютерні науки та кібербезпека*. 2021. № 2. С. 45 – 56. URL: https://periodicals.karazin.ua/cscs/article/view/18183 (дата звернення: 01.11.2022).
3. Гончаров М. О., Малахов С. В. Моделювання процедур підготовки даних стеганоалгорітма з багаторівневим мультиплексуванням контенту. *Комп'ютерне моделювання в наукоємних технологіях (КНМТ-2021)* : матеріали 7-ї міжнар. наук.-техн. конф., 21-23 квіт. 2021 р. Харків : ХНУ ім. В.Н. Каразіна. – URL: http:// www-csd.univer.kharkov.ua/wp-content/uploads/2018/02/www csd.univer.kharkov.ua -maket-pdf-konf.pdf (дата звернення: 01.11.2022).
4. Дослідження параметру «серій опорних блоків», як елементу композитного ключа екстрактора даних стеганоалгоритму / Гончаров М. О. та ін. *Problems of science and practice, tasks and ways to solve them* : матеріали 20-ї міжнар. наук.-техн. конф., 24–27 трав. 2022 р. м. Варшава, Польща. С. 779 – 785. – URL: https://isg-konf.com/wp-content/uploads/2022/05/Problems-of-science-and-practice-tasks-and-ways-to-solve-them.pdf (дата звернення 01.11.2022).

5. Гончаров М. О. Дослідження процедур попередньої підготовки вихідних даних для стеганоалгоритма. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : матеріали 11-ї міжнар. наук.-техн. конф., 8–9 квіт. 2021 р. м. Баку–Харків–Київ–Жиліна. т. 2. с. 63. – URL: http://repository.kpi.kharkov.ua/handle/KhPI-Press/52020 (дата звернення 01.11.2022).
6. Гончаров М. О. Моделювання та дослідження властивостей гібридного внутрікадрового стеганоалгоритму: Пояснювальна записка до дипломної роботи бакалавра: напрям підготовки 125 – Кібербезпека / М. О. Гончаров; Харківський національний університет імені В. Н. Каразіна. – Харків: [Б. В.], 2021. – 75 с.
7. Результаты атаки стеганоконтента при разной ширине стека выборки серий на этапе межблочного мультиплекса данных / Гончаров Н. А. та ін. *Current trends in the development of modern scientific thought* : матеріали 1-ї міжнар. наук.-техн. конф., 27–30 верес. 2022 р. м. Хайфа, Ізраїль. С. 465–471. – URL: https://doi.org/10.46299/ISG.2022.2.1 (дата звернення 04.11.2022).
8. Гончаров Н. А, Малахов С. В. Использование параметра длин серий, как элемента межблочного мультиплекса данных стеганоалгоритма. *Débats scientifiques et orientations prospectives du développement scientifique* : матеріали 3-ї міжнар. наук.-техн. конф., 8 лип. 2022 р. м. Париж, Франція. С. 180 – 187. – URL: https://doi.org/10.36074/logos-08.07.2022.050 (дата звернення 04.11.2022).
9. Гончаров Н.А., Лесная Ю.Е., Малахов С.В. Результаты внутриблочного мультиплексирования параметра средней яркости опорных блоков стеганоконтента наразной базе перестановок. *Débats scientifiques et orientations prospectives du développement scientifique* : матеріали 4-ї міжнар. наук.-техн. конф., 11 лист. 2022 р. м. Париж, Франція. С. 78 – 81. – URL: https://archive.logos-science.com/index.php/conference-proceedings/issue/view/6/6 (дата звернення 11.11.2022).

10. Гончаров Н. А., Лесная Ю. Е., Малахов С. В. Моделирование атаки стеганоконтента при грубых оценках подобия исходных данных и разной базе стека выборки серий. *Scientific practice: modern and classical research methods* : матеріали 3-ї міжнар. наук.-техн. конф., 16 вер. 2022 р. м. Бостон, USA. С. 86 – 90. – URL: https://doi.org/10.36074/logos-16.09.2022.23 (дата звернення 04.11.2022).
11. Гончаров Н. А., Лесная Ю. Е., Малахов С. В. Адаптация принципа кодирования длин серий для противодействия попыткам неавторизованной экстракции стеганоконтента. *Grail of Science*. 2022. № 17. С. 241–247. URL: https://doi.org /10.36074/grail-of-science.22.07.2022.042 (дата звернення: 04.11.2022).
12. Гончаров М. О., Лєсная Ю. Є., Малахов С. В. Моделювання спроб екстракції стеганоконтента при різній довжині стеку вибірки параметрів серій. *Grail of Science*. 2022. № 18-19. С. 173–177. https://doi.org/10.36074/grail-of-science. 26.08.2022.31 (дата звернення: 04.11.2022).
13. Гончаров Н. А., Малахов С. В. Результаты моделирования межблочного мультиплекса параметров длин серий для противодействия попыткам неавторизованного извлечения стеганоконтента. *The newest problems of science and ways to solve them* : матеріали 30-ї міжнар. наук.-техн. конф., 2–5 серп. 2022 р. м. Гельсінкі, Фінляндія. С. 248 - 250. – URL: https://doi.org/10.46299/ ISG.2022.1.30 (дата звернення 08.11.2022).
14. Гончаров М. О. Результати моделювання процедур багаторівневого мультиплексу даних гібридного стеганоалгоритму. *Концепт науки XXI: стратегії, методи та наукові інструменти* : матеріали 2-ї міжнар. студ. наук. конф., 22 жовт. 2022 р. м. Черкаси. С. 155 - 157. – URL: https://doi.org/10.36074/liga-inter-21.10.2022 (дата звернення 08.11.2022).

15. Лєсная Ю. Є., Гончаров М. О., Малахов С. В. Моделювання короткого стеку вибірки довжин серій при різних комбінаціях параметрів мультиплексування. *Multidisciplinary scientific notes. Theory, history and practice* : матеріали 6-ї міжнар. наук.-техн. конф., 1–4 лист. 2022 р. м. Едмонтон, Канада. С. 684 - 687. – URL: https://doi.org/10.46299/ISG. 2022.2.6 (дата звернення 08.11.2022).
16. Ярославский Л.П. Введение в цифровую обработку изображений. М.: Сов.Радио, 1979. – 312 с.
17. Подвійна обфускація трансформант малоресурсного стеганоалгоритма / Морозов Д. та ін. *Комп'ютерні науки та кібербезпека*. 2018. № 1. С. 22–34. URL: https://periodicals.karazin.ua/cscs/article/view/12015 (дата звернення: 13.11.2022).
18. Моделирование атаки стеганоконтента на коротком стеке выборки параметров серийпри грубых оценках подобия исходных данных / Гончаров Н. А. та ін. *The main prospects for the development of science in modern life* : матеріали 36-ї міжнар. наук.-техн. конф., 13–16 верес. 2022 р. м. Варшава, Польща. С. 344 – 347. – URL: https://www.doi.org/10.46299/ISG.2022.1.36 (дата звернення 1.05.2021).
19. Прэтт У. Цифровая обработка изображений / пер. с англ. Д. С. Лебедева. т. 1,2. Москва: Мир, 1985. 736 с.
20. Зубарев Ю. Б., Дворкович В. П. Цифровая обработка телевизионных и компьютерных изображений. Москва : МЦНТИ, 1997. 212 с.
21. Бутаков Е. А., Островский В. И., Фадеев И. Л. Обработка изображений на ЭВМ. Москва : Радио и связь, 1987. 240 с.
22. Королев А. В. Оценка информативности трансформант дискретного косинусного преобразования. *Системи Обробки Інформації*. 2003. № 3. С. 81-86.
23. Красильников Н.Н. Статистическая теория передачи изображений.- М.: Связь, 1976.- 184 с.

24. Гончаров М., Лєсная Ю. Використання параметрів довжин серій, як елемента міжблочного мультиплексу даних стеганоалгоритму. *Комп'ютерні науки та кібербезпека*. 2022. № 1. С. 30 – 39. URL: https://periodicals.karazin.ua/cscs/article/view/20911 (дата звернення: 15.11.2022).
25. Гончаров Н. А., Лесная Ю. Е., Малахов С. В. Результаты неавторизованного извлечения стеганоконтента при разной длине стека выборки длин серий. *Trends in the development of science in the modern world* : матеріали 33-ї міжнар. наук.-техн. конф., 23-26 серп. 2022 р. м. Грац, Австрія. С. 391 – 396. – URL: https://doi.org/10.46299/ISG.2022.1.33 (дата звернення 16.11.2022).

ДОДАТОК А

Публікації та апробації на конференціях

Сертифікат

учасника І міжнародної науково-теоретичної конференції

CURRENT ISSUES OF SCIENCE, PROSPECTS AND CHALLENGES

Рисунок А.1 – Сертифікат участника (публікації) конференції [1].

I Міжнародна науково-теоретична конференція

CURRENT ISSUES OF SCIENCE, PROSPECTS AND CHALLENGES

Рисунок А.2 – Обкладинка збірника статей за матеріалами конференції [1].

Current issues of science, prospects and challenges | Volume 2

Лесная Юлия Евгеньевна
студентка факультета компьютерных наук (*бакалавриат*)
Харьковский национальный университет имени В. Н. Каразина, Украина

Гончаров Никита Александрович
студент факультета компьютерных наук (*магистратура*)
Харьковский национальный университет имени В. Н. Каразина, Украина

Малахов Сергей Витальевич
канд. техн. наук, старший научный сотрудник,
доцент кафедры безопасности информационных систем и технологий
Харьковский национальный университет имени В. Н. Каразина, Украина

ОТРАБОТКА КОНЦЕПТА МНОГОУРОВНЕВОГО МУЛЬТИПЛЕКСА ДАННЫХ ГИБРИДНОГО СТЕГАНОАЛГОРИТМА

Аннотация. *Рассмотрены вопросы реализации процедур предварительной обработки и последующей инкапсуляции контента (изображений), в рамках моделирования основных этапов гибридного стеганографического алгоритма. Тестовая модификация алгоритма обеспечивает необходимое препарирование и подготовку данных контейнера и контента, с последующим многоуровневым мультиплексом данных, формирующих основные позиции в структуре составного ключа экстрактора. Основные процедуры выполнены в версии «лайт», как демонстратор возможностей общей концепции.*

Введение.

Решение вопросов обеспечения оперативной и малоресурсной (*малой вычислительной сложности*) стегановставки с требуемыми показателями скрытности факта инкапсуляции данных и стойкости к попыткам нелегитимной экстракции скрытого контента, является актуальной задачей. Исследуемый прототип гибридного алгоритма использует различные свойства, эффекты и методы кодирования видеоданных. Выбранная концепция алгоритма обеспечивает широкий диапазон комбинаторики выделяемых параметров кодирования (*и для контейнера и для контента*), что потенциально расширяет вариативность реализаций структуры составного ключа экстрактора данных.

Основная часть.

В данной работе представлены некоторые результаты моделирования основных процедур обработки данных в рамках тематики создания прототипа гибридного стеганографического алгоритма обработки изображений. В своей структуре, алгоритм имеет четыре основных функциональных модуля, последовательно реализующих все предусмотренные этапы обработки данных.

Состав основных этапов (*для действующего релиза прототипа*) имеет следующий вид [1-6]:

1 – предварительная подготовка (*анализ и сглаживание*) исходных данных;

2 – формирование серий подобных (*т.е. идентичных по заданным критериям*) блоков изображений;

3 – обработка опорных блоков сформированных серий, посредством применения методов кодирования с преобразованием (*в данном случае дискретного косинусного преобразования*) с последующей селекцией и квантованием всех сохраняемых коэффициентов трансформант;

Рисунок А.3 – Перша сторінка доповіді [1], с.48.

КОМП’ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

COMPUTER SCIENCE AND CYBERSECURITY (CS&CS)

Рисунок А.4 – Обкладинка журналу [2].

ISSN 2519-2310 CS&CS, Issue 2(20) 2021

УДК 621.327:621.391 DOI: 10.26565/2519-2310-2021-2-05

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ПРОТОТИПУ ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ

Микита Гончаров, Юлія Лєсная, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
worldxdark@gmail.com, xa12284109@student.karazin.ua, mailgate@meta.ua

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологічний університет Монтеррея, 64849 Монтеррей, Нуево-Леон, Мексика
kalash@itesm.mx

Надійшла: Листопад 2021.

***Анотація**: Метою даного матеріалу є ознайомлення з основними етапами адаптивного малоресурсного алгоритму стеганографічної обробки зображень і результатами моделювання процедур попередньої обробки вихідних даних різних типів. Процедури імітаційного алгоритму дозволяють: - враховувати особливості оброблюваних даних (типи контейнера і контенту) і коригувати параметри роботи основних модулів стеганоалгоритму (модуль попередньої обробки вхідних даних та модуль спеціальних перетворення). Досліджено інші параметри обробки зображень, які безпосередньо впливають на обчислювальну складність 1-го етапу алгоритму (згладжування) та якість візуалізації контейнера та вмісту. Зазначено, що для всіх типів зображень, варіант попереднього згладжування вхідних блоків, за принципом «перебір всіх з усіма», надає кращі результати. В даному випадку, зі зменшенням розмірності матриць згладжування, інтенсивність візуально помітних аномалій зменшується.*

Підкреслено, що при збільшені значення порога загрублення яскравості елементів (P_Z), кількість і помітність артефактів зростає. Зростання фіксується для всіх типів зображень і всіх варіантів їх попереднього згладжування. Стійке зростання викривлень відбувається при виборі значень P_Z більш 7. Для реалістичних зображень, критично припустимою слід вважати величину $P_Z = 14$. Звернено увагу на те, що в незалежності від встановлених значень P_Z та обраного варіанту згладжування, візуальна помітність викривлень, посилюється в наступній послідовності: «портрет – пейзаж – мнемосхема». Найбільш «чутливими» до варіантів попереднього згладжування, виявилися зображення типу «мнемосхема». Це можна пояснити чутливістю контурів до їх найменших змін та особливостями структури таких зображень.

Звернено увагу на те, що факт малої обчислювальної складності процедур попередньої обробки зображень, є принциповим з урахуванням концепції створення мобільних додатків. Зроблено висновок, що потенційний виграш від введення етапу попередньої обробки вихідних даних, дозволяє отримати 3 важливі ефекти: 1 - знизити обчислювальну складність алгоритму; 2 - використовувати різні принципи обробки даних контейнера та контенту; 3 - створити необхідні умови для асиметричного режиму обробки даних контейнера та контенту.

***Ключові слова:** зображення; стеганографія; кодування з перетворенням; контейнер; контент; згладжування зображень; візуальна помітність викривлень; кодування серій; мультиплексування.*

1 Вступ

Добре відомо, що одним із ефективних напрямів забезпечення приховування фактів передачі і зберігання інформації, є застосування різних стеганографічних методів [1]. Цифрова стеганографія, як окремий науковий напрямок, вивчає можливості використання властивостей цифрового контенту різного типу для забезпечення більш ефективного вирішення завдань, які пов'язані с синтезом нових методів і способів прихованої передачі, зберігання та маркування цільової інформації (*надалі контенту*). Принциповим є те, що в незалежності від використаного напрямку стеганографії, необхідно забезпечувати мінімізацію демаскуючих аномалій використовуваних контейнерів та підтримувати заданий рівень стійкості контенту стовно спроб його неавторизованої екстракції, а в деяких випадках, і стійкості до спроб навмисного спотворення контейнерів.

2 Основна частина

При приховувані в цифрових об'єктах будь-якої іншої – корисної інформації, нажаль, виникають певні спотворення цих об'єктів – переносників даних [1]. При збалансованих налаштуваннях відповідного стеганоалгоритму, можливо забезпечувати рівень спотворень кон-

Рисунок А.5 – Перша сторінка статті [2], с. 45.

Сертифікат

Учасника науково-технічної міжнародної конференції

«Комп’ютерне моделювання в наукоємних технологіях (КМНТ-2021)»

Рисунок А.6 – Сертифікат участника (публікації) конференції [3].

УДК 621.327:621.391 **СЕКЦІЯ 5**

ГОНЧАРОВ М.О, МАЛАХОВ С.В.

МОДЕЛЮВАННЯ ПРОЦЕДУР ПІДГОТОВКИ ДАНИХ СТЕГАНОАЛГОРІТМА З БАГАТОРІВНЕВИМ МУЛЬТИПЛЕКСУВАННЯМ КОНТЕНТУ

Введення

Добре відомо, що одним із ефективних напрямів забезпечення приховування фактів передачі і зберігання інформації, є застосування різних стеганографічних методів [1]. Цифрова стеганографія, як окремий науковий напрямок, вивчає можливості використання властивостей цифрового контенту різного типу для забезпечення більш ефективного вирішення завдань, які пов'язані с синтезом нових методів і способів прихованої передачі, зберігання та маркування цільової інформації (надалі контенту). Принциповим є те, що в незалежності від використаного напрямку стеганографії, необхідно забезпечувати мінімізацію демаскуючих аномалій використовуваних контейнерів та підтримувати заданий рівень стійкості контенту стовно спроб його неавторизованої екстракції, а в деяких випадках, і стійкості до спроб навмисного спотворення контейнерів.

Основна частина

При приховувані в цифрових об'єктах будь-якої іншої – корисної інформації, нажаль, виникають певні спотворення цих об'єктів – переносників даних [1]. При збалансованих налаштуваннях відповідного стеганоалгоритму, можливо забезпечувати рівень спотворень контейнерів, які знаходяться нижче порога чутливості зорової системи людини [2] або чутливості його слухової системи, що забезпечує фактичну відсутність візуально або аудіо помітних змін (аномалій) переносників інформації (контейнерів). Тим самим забезпечується необхідний баланс між збереженням характерних властивостей для використовуваного типу контейнерів (у нашому випадку, напівтонових зображень [2]), та величиною допустимих спотворень, прийнятних для заданого типу прихованого контенту (в даному випадку зображень з різною вірогідністю перепаду яскравості між сусідніми елементами). В цьому сенсі зрозуміло, що кількість і інтенсивність проявів різних артефактів зображень контейнеру і контенту, знаходяться в прямій залежності від коректності обраних для них режимів обробки. При цьому, слід мати на увазі, що при обробці даних контейнерів і контенту можуть бути використані, як однотипні (симетричні) режими обробки, так і режими, які реалізують різні параметри обробки даних (асиметричні). Такими відмінностями можуть бути: – відмінності в розмірах блоків; – відмінності в параметрах попередньої обробки масивів даних контейнерів і контенту (що є головним змістом даного матеріалу); – відмінності в критеріях оцінки значущої інформації контейнерів і контенту; – відмінності реалізацій прискорення обчислювальних процедур та інше. Таким чином, на одних і тих же типах даних (в даному випадку зображень) можна отримати різний ефект, з точки зору помітності артефактів, що зменшує зайвий привід задуматися про причини появи цих аномалій даних [1-2].

В основу дослідного алгоритму положено принцип внутрішньо-кадрового стиснення зображень, який передбачає послідовне використання двох різних методів: 1 - методу кодування довжин серій [3, 4]; 2 - методу кодування з перетворенням, а саме ДКП (дискретного косинус перетворення) [2, 4]. Використання властивостей ДКП дозволяє «вбудовувати» контент в матриці коефіцієнтів перетворення контейнерів, визначених алгоритмом попередньої обробки, як опорний блок (тобто перший в серії подібних). Процедура інкапсуляції стеганоконтенту має два рівня реалізації – внутрішньоблоковий та міжблоковий. Перший рівень реалізується за результатами проведення селекції коефіцієнтів перетворення [4-5] для контейнера і контенту (можливі відмінності в параметрах обробки). На кожному з цих рівнів здійснюється змішування коефіцієнтів (на 1-му рівні) або блоків (на 2-му рівні) у відповідності з маскою мультиплексування, яка притаманна для кожного з рівнів обробки. Використання методів кодування з перетворенням забезпечує отримання матриць спектральних коефіцієнтів,

Рисунок А.7 – Перша сторінка доповіді [3], с.118.

Сертифікат

учасника XX міжнародної науково-практичної конференції

PROBLEMS OF SCIENCE AND PRACTICE, TASKS AND WAYS TO SOLVE THEM

Рисунок А.8 – Сертифікат за участь у роботі конференції [4].

XX Міжнародна науково-практична конференція

PROBLEMS OF SCIENCE AND PRACTICE, TASKS AND WAYS TO SOLVE THEM

Рисунок А.9 – Обкладинка збірника статей з матеріалами конференції [4].

ДОСЛІДЖЕННЯ ПАРАМЕТРУ «СЕРІЙ ОПОРНИХ БЛОКІВ», ЯК ЕЛЕМЕНТУ КОМПОЗИТНОГО КЛЮЧА ЕКСТРАКТОРА ДАНИХ СТЕГАНОАЛГОРИТМУ

Гончаров Микита Олександрович
студент факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Лєсная Юлія Євгеніївна
студентка факультету комп'ютерних наук, (бакалавріат)
Харківський національний університет імені В.Н. Каразіна, Україна

Погоріла Каріна Валеріївна
студентка факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Богданова Єлизавета Сергіївна
студентка факультету комп'ютерних наук, (бакалавріат)
Харківський національний університет імені В.Н. Каразіна, Україна

Малахов Сергій Віталійович
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, Україна

Вирішення питань забезпечення оперативної і малоресурсної стегановставки (*малої обчислювальної складності використовуваного алгоритму*) з необхідними показниками скритності факту інкапсуляції даних, та стійкості до спроб нелегітимної екстракції прихованого контенту є актуальним завданням. У цій роботі стисло представлені деякі результати моделювання процедур формування серій опорних блоків (*класифікованих, як блоки з ідентичним змістом*), що є одним з важливих етапів створюваного концепту гібридного алгоритму стеганографічного обробки зображень.

Попередньо, дослідний алгоритм має чотири основні функціональні модулі, що послідовно реалізують всі передбачені етапи обробки даних [1-3].

Склад основних етапів алгоритму (*для чинного релізу*) має такий вигляд:

1 – попередня підготовка (*аналіз та згладжування*) вихідних даних [1];

2 – формування серій подібних (*ідентичних за заданими критеріями*) блоків зображень [3-4];

3 – обробка кожного першого блоку в кожній із сформованих серій (надалі опорних блоків - ОБ), за допомогою методів кодування з перетворенням з подальшою селекцією та квантуванням всіх збережених коефіцієнтів трансформант [5-7];

Рисунок А.10 – Перша сторінка доповіді [4], с.779.

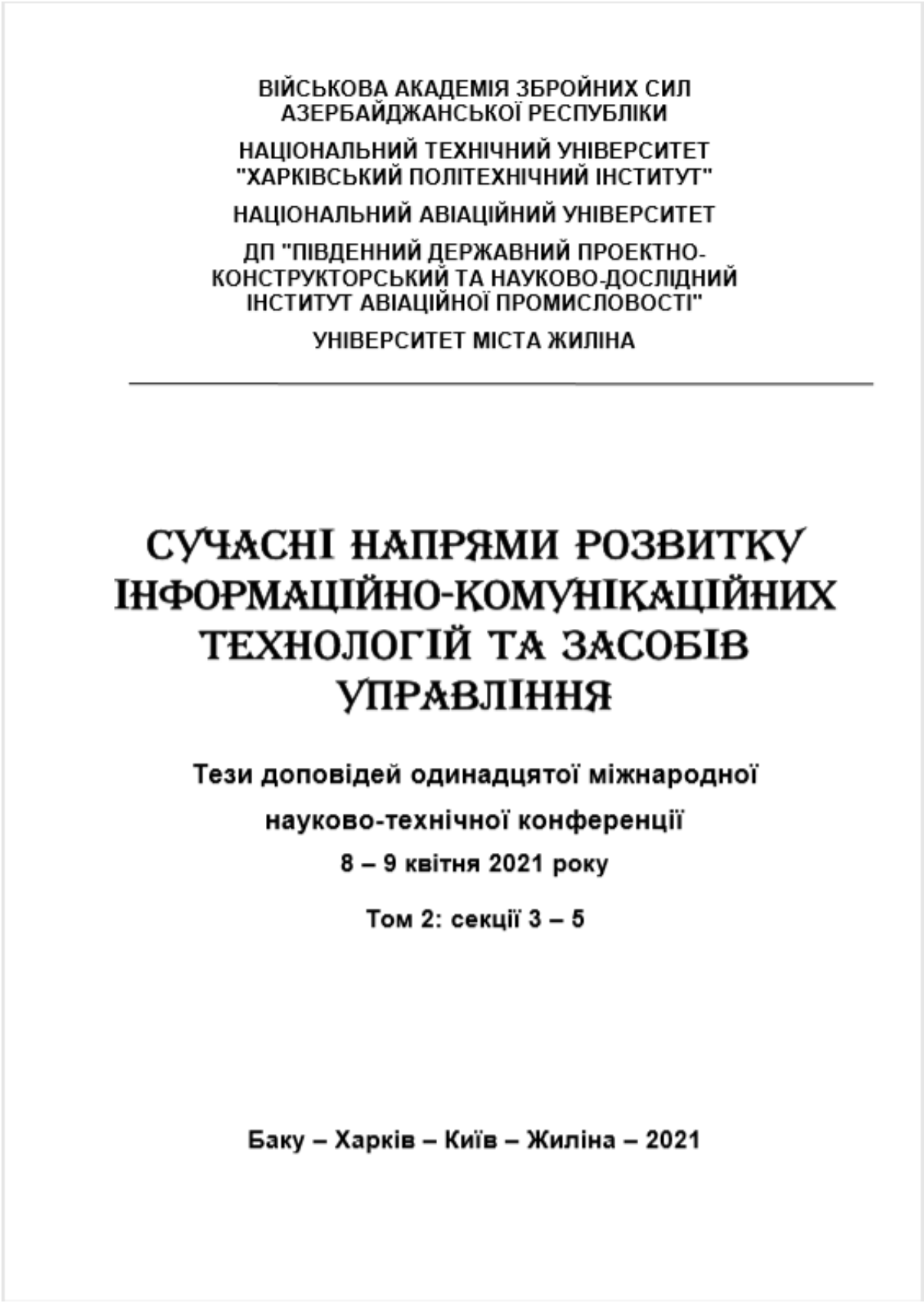


Рисунок А.11 – Обкладинка збірника тез [5].

ДОСЛІДЖЕННЯ ПРОЦЕДУР ПОПЕРЕДНЬОЇ ПІДГОТОВКИ ВИХІДНИХ ДАНИХ ДЛЯ СТЕГАНОАЛГОРИТМА

Гончаров М.О.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Розглянуто питання попередньої обробки відеоданих, які забезпечують необхідні умови для поліпшення параметрів вставки приховуваного контенту при реалізації основних процедур дослідного стеганоалгорітма [1].

Метою доповіді є розгляд результатів моделювання процедур перетворень структури вхідних даних (потенційного контейнеру, та безпосередньо, зображення-контенту), що дозволяють забезпечити необхідні умови для одночасного вирішення двох завдань: - скорочення часу обробки (зменшення обчислювальної складності алгоритму); - ускладнення процедур аналізу і неавторизованої екстракції прихованого контенту.

Основним завданням етапу попередньої обробки даних, є зменшення кількості візуально малопомітних перепадів яскравості елементів вихідних зображень [2-3].

В цілому, ця процедура зводиться до реалізації згладжування малоінформативних областей зображень. Причому, в залежності від складності структури оброблюваних зображень (в даному випадку, значень ймовірності перепаду яскравості між сусідніми елементами [3]), параметри обробки можуть змінюватися.

Наведено результати моделювання для блоків розмірністю 3×3 елемента. Зазначено, що згладжене, зображення, формується шляхом циклічного повторення спеціальних процедур обробки, що застосовані до всього масиву вихідних даних (контейнера і контенту). Досліджено три варіанти реалізація процедур згладжування, з різним порядком взаємного порівняння складових елементів блоку, та різним способом перезапису їх змісту, при перевищенні заданих критеріїв подібності (відповідно для зображень контейнера і контенту).

Підкреслено важливість фактів локалізації присутності контурів та розглянуто можливість застосування симетричної і несиметричної предобробки вхідних масивів даних. Звернено увагу на те, що використовуваний механізм обробки характеризується простотою і забезпечує необхідні «стартові» умови для подальшого інкапсуляції стеганоконтента.

Список літератури

1. Morozov, D., Shaforostov, M., Malakhov, S., & Serbin, V. (2018). Подвійна обфускація трансформант малоресурсного стеганоалгоритма. Комп'ютерні науки та кібербезпека, 9(1), 22-34. Retrieved is https://periodicals.karazin.ua/cscs/article/view/12015

2. Зубарев Ю.Б., Дворкович В.П. Цифровая обработка телевизионных и компьютерных изображений. – М.: МЦНТИ, 1997. – 212 с.

3. Прэтт У. Цифровая обработка изображений. т.1,2. - М.: Мир, 1985. - 736 с.

Рисунок А.12 – Перша сторінка тез [5], с. 63.

Сертифікат

учасника I міжнародної науково-практичної конференції

CURRENT TRENDS IN THE DEVELOPMENT OF MODERN SCIENTIFIC THOUGHT

Рисунок А.13 – Сертифікат участника (публікації) конференції [7].

І Міжнародна науково-практична конференція

CURRENT TRENDS IN THE DEVELOPMENT OF MODERN SCIENTIFIC THOUGHT

Рисунок А.14 – Обкладинка збірника статей з матеріалами конференції [7].

РЕЗУЛЬТАТЫ АТАКИ СТЕГАНОКОНТЕНТА ПРИ РАЗНОЙ ШИРИНЕ СТЕКА ВЫБОРКИ СЕРИЙ НА ЭТАПЕ МЕЖБЛОЧНОГО МУЛЬТИПЛЕКСА ДАННЫХ

Гончаров Никита Александрович
студент факультета компьютерных наук (магистратура)
Харьковский национальный университет имени В. Н. Каразина, Украина

Лесная Юлия Евгеньевна
студентка факультета компьютерных наук (магистратура)
Харьковский национальный университет имени В. Н. Каразина, Украина

Семёнов Артём Сергеевич
студент факультета радиоэлектроники, компьютерных систем и инфокоммуникаций (бакалавриат)
Национальный аэрокосмический университет им. М.Е. Жуковского, "ХАИ", Украина

Малахов Сергей Витальевич
канд. техн. наук, ст. науч. сотрудник, доцент кафедры
Харьковский национальный университет имени В. Н. Каразина, Украина

Представленные результаты являются логическим продолжением цикла работ, в рамках отработки общей концепции по созданию малоресурсного гибридного стеганоалгоритма, реализующего несколько процедурных уровней защиты контента [1-3]. Целью данного материала является краткое ознакомление с результатами моделирования попыток несанкционированного извлечения стеганоконтента (*в данном случае, полутоновых изображений*), защищаемого посредством реализации механизма межблочного мультиплексирования действующих параметров массива длин серий, сформированного по результатам обработки исходных тестовых изображений, в условиях использования короткого и длинного стеков выборки серий [2,4].

На этапе предобработки исходных данных (*контента*) использовался вариант сглаживания представленный на рис.1(а) в работе [1]. Размер «окна сглаживания» фиксировался размерностью 3×3 эл., что потенциально уменьшает величину вносимых искажений исходных данных. Последующее формирование базового массива серий опорных блоков (ОБ) производилось для двух разных размерностей ОБ: - 4×4 и 8×8 эл. Величина допустимой разницы значений яркости элементов в соседних блоках изображений (*Pz*) на этапе формирования массива серий ОБ, фиксировалась значением в 7 градаций, что приемлемо [3, 5] при обработке тестовых изображений выбранного типа.

Для формирования базового массива серий ОБ, использовались разные способы их развертки. Изменение способа развертки серий имитирует *различные*

Рисунок А.15 — Перша сторінка доповіді [7], с.465.

Сертифікат

учасника III міжнародної науково-практичної конференції

DÉBATS SCIENTIFIQUES ET ORIENTATIONS PROSPECTIVES DU DÉVELOPPEMENT SCIENTIFIQUE

Рисунок А.16 – Сертифікат участника (публікації) конференції [8].

III Міжнародна науково-практична конференція

DÉBATS SCIENTIFIQUES ET ORIENTATIONS PROSPECTIVES DU DÉVELOPPEMENT SCIENTIFIQUE

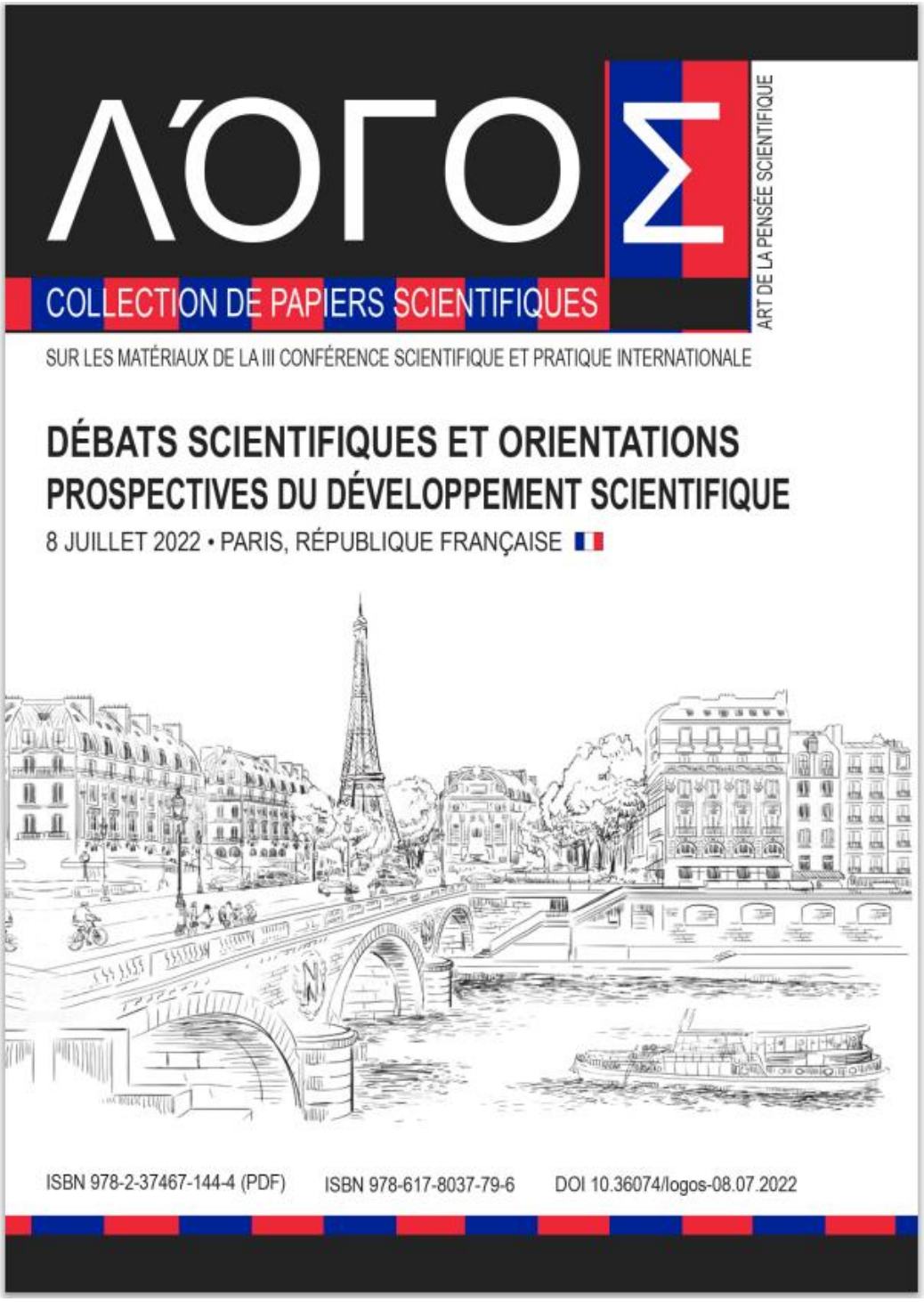


Рисунок А.17 – Обкладинка збірника статей з матеріалами конференції [8].

DOI 10.36074/logos-08.07.2022.050

ИСПОЛЬЗОВАНИЕ ПАРАМЕТРА ДЛИН СЕРИЙ, КАК ЭЛЕМЕНТА МЕЖБЛОЧНОГО МУЛЬТИПЛЕКСА ДАННЫХ СТЕГАНОАЛГОРИТМА

ORCID ID: 0000-0002-9790-7260 **Гончаров Никита Александрович**
студент факультета компьютерных наук (*магистрант*)
Харьковский национальный университет имени В. Н. Каразина

ORCID ID: 0000-0001-8826-1616 **Малахов Сергей Витальевич**
канд. техн. наук, ст. науч. сотрудник,
доцент кафедры безопасности информационных систем и технологий
Харьковский национальный университет имени В. Н. Каразина

УКРАИНА

***Аннотация**. Рассмотрены особенности использования параметра длин серий и количества сформированных опорных блоков, как элементов составного ключа экстрактора данных гибридного стеганоалгоритма. Представлены результаты атаки (взлома) тестовых изображений для различных комбинаций мультиплекса ключевых параметров на коротком стеке (малой базе перестановок). Сделан вывод о ведущей роли параметра длин серий при реализации процедур межблочного мультиплекса стеганоконтента.*

Введение. Данная работа отражает некоторые результаты, полученные в ходе проведения моделирования основных процедур межблочного мультиплексирования данных, в рамках реализации общей концепции [1] малоресурсного гибридного стеганографического алгоритма. Основное внимание уделено исследованию получаемых эффектов, при использовании в качестве элементов составного ключа экстрактора данных, следующих двух параметров: – количества опорных блоков изображений [2] и параметра длин серий опорных блоков (ОБ). Формирование серий ОБ, является следствием проведения специальных процедур «сглаживания» (*предобработки*) исходных изображений, реализованных на предыдущем этапе алгоритма [1].

В рамках моделирования основных процедур предобработки рассмотрены три способа сглаживания изображений [1], позволяющие получить требуемый результат [2] по количеству формируемых блоков идентичного содержания, для различных типов исходных данных (*в данном случае изображений*).

В качестве тестовых образцов, использованы полутоновые изображения трех разных типов: - изображение типа «*портрет*»; - изображение типа «*лейзаж*» и изображение типа «*мнемосхема*». Основное отличие между ними заключается в характерных значениях вероятности перепада яркости, между соседними элементами изображений каждого типа [3,4].

Основная часть.

Для демонстрации полученных эффектов, использована «*лайт*» версия тестового алгоритма, ограниченная мультиплексированием 2-х элементов (*количества ОБ и длин серий*) составного ключа экстрактора, формирующих межблочный уровень комбинаторики параметров стегановставки. Для условной нормировки представленных результатов были использованы одинаковая

Рисунок А.18 — Перша сторінка доповіді [8], с.180.

Сертифікат

учасника IV міжнародної науково-практичної конференції

DÉBATS SCIENTIFIQUES ET ORIENTATIONS PROSPECTIVES DU DÉVELOPPEMENT SCIENTIFIQUE

Рисунок А.19 – Сертифікат участника (публікації) конференції [9].

IV Міжнародна науково-практична конференція

DÉBATS SCIENTIFIQUES ET ORIENTATIONS PROSPECTIVES DU DÉVELOPPEMENT SCIENTIFIQUE

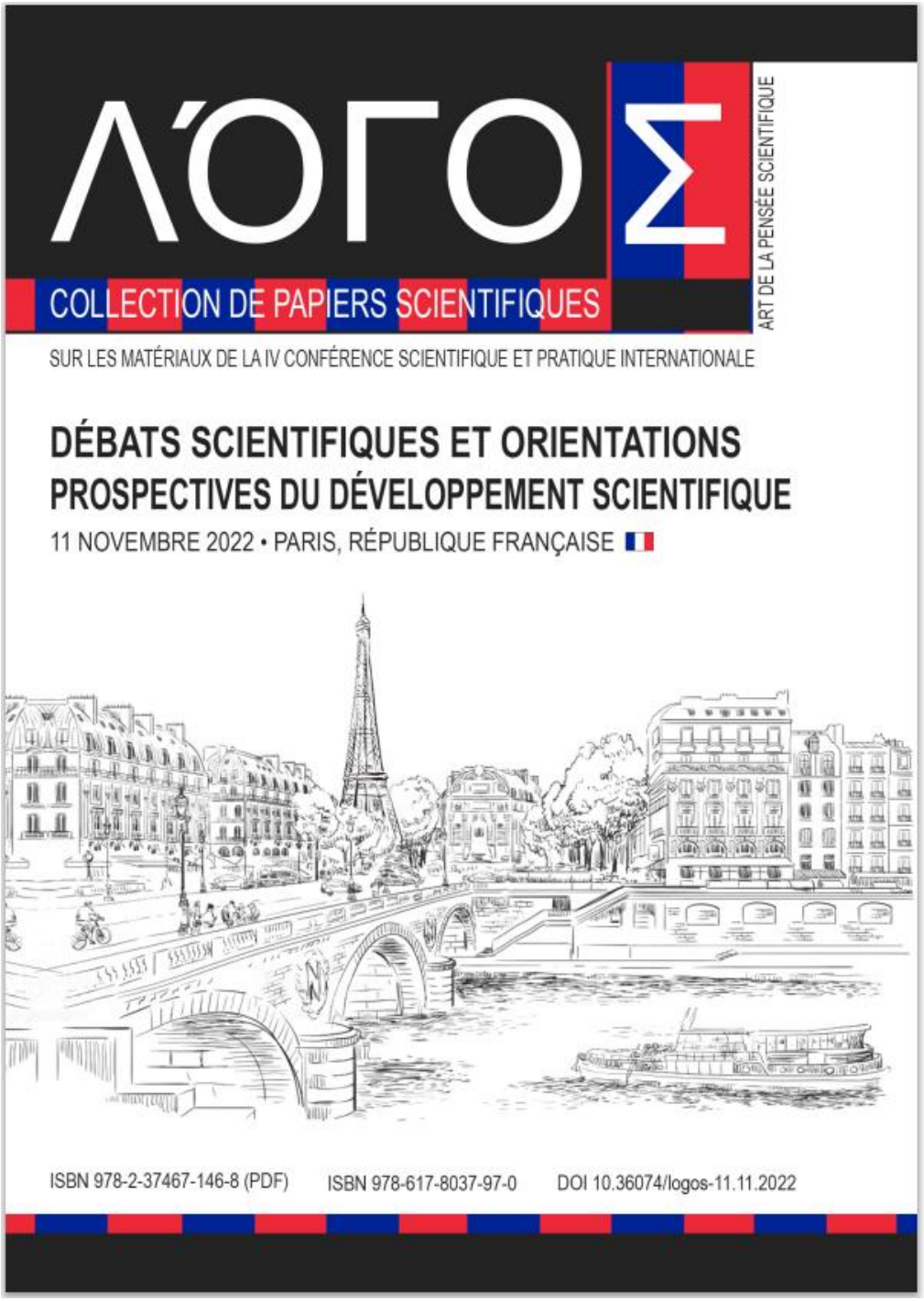


Рисунок А.20 –Обкладинка збірника статей з матеріалами конференції [9].

DOI 10.36074/logos-11.11.2022.21

РЕЗУЛЬТАТЫ ВНУТРИБЛОЧНОГО МУЛЬТИПЛЕКСИРОВАНИЯ ПАРАМЕТРА СРЕДНЕЙ ЯРКОСТИ ОПОРНЫХ БЛОКОВ СТЕГАНОКОНТЕНТА НА РАЗНОЙ БАЗЕ ПЕРЕСТАНОВОК

ORCID ID: 0000-0002-9790-7260 **Гончаров Никита Александрович**
студент факультета компьютерных наук (*магистратура*)
Харьковский национальный университет имени В. Н. Каразина

Лесная Юлия Евгеньевна
студентка факультета компьютерных наук (*магистратура*)
Харьковский национальный университет имени В. Н. Каразина

ORCID ID: 0000-0001-8826-1616 **Малахов Сергей Витальевич**
канд. техн. наук, старший научный сотрудник,
доцент кафедры безопасности информационных систем и технологий
Харьковский национальный университет имени В. Н. Каразина

УКРАИНА

Вступление.
В работе представлены результаты моделирования атаки стеганоконтента, противостоящего попыткам его несанкционированного извлечения из контейнера, посредством реализации процедур 2-х уровневого мультиплексирования действующих параметров серий опорных блоков (ОБ) тестовых изображений. Основное внимание уделено демонстрации результатов, атаки контента, защита которого была ограничена на уровне процедур внутриблочного мультиплекса. Такая концепция эксперимента позволила визуализировать последствия «работы» данного уровня защиты, имитируя ситуацию успешного подбора атакующим текущих параметров маски межблочного мультиплексирования параметров серий ОБ.

Основная часть. Для демонстрации получаемых эффектов в тестовой версии исследовательского алгоритма [1], предусмотрена возможность избирательного «отключения» любого из 2-х этапов обработки контента:

1 – процедур ***внутриблочного*** мультиплексирования коэффициентов трансформант, характеризующих среднюю яркость сформированных ОБ (*элементы (0;0) на рис.1 в работе [2]*), полученных по результатам реализации кодирования с преобразованием (*в данном случае - дискретное косинусное преобразование*) [3]. Т.е. в данном случае защита контента обеспечивается реализацией процедур на уровне межблочного мультиплексирования;

2 - процедур ***межблочного*** мультиплексирования действующих параметров длин серий ОБ [2]. На рис.1, данная операция соответствует 4-му шагу алгоритма *(Multiplex Level 1)*. Т.о., в данном случае защита контента ограничена только уровнем процедур внутриблочного мультиплекса.

Таким образом, шаг №4 (*«Multiplex Level 1»*), соответствует режиму межблочной обработки, а шаг №6 (*«Multiplex Level 2»*), режиму внутриблочного мультиплексирования действующих параметров контента.

Рисунок А.21 — Перша сторінка доповіді [9], с.78.

Сертифікат

учасника III міжнародної науково-практичної конференції

SCIENTIFIC PRACTICE: MODERN AND CLASSICAL RESEARCH METHODS

Рисунок А.22 – Сертифікат участника (публікації) конференції [10].

III Міжнародна науково-практична конференція

SCIENTIFIC PRACTICE: MODERN AND CLASSICAL RESEARCH METHODS

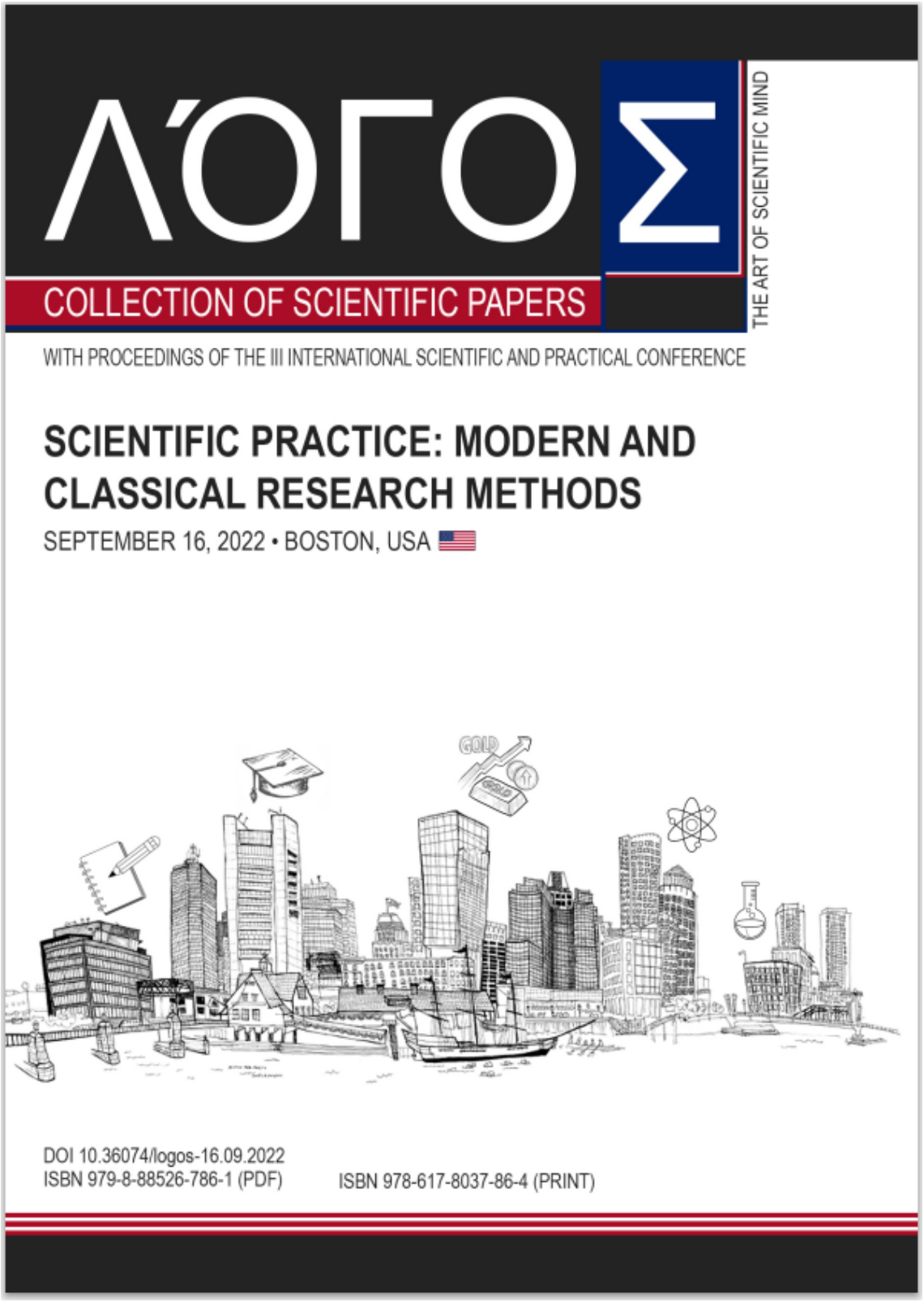


Рисунок А.23 – Обкладинка збірника статей з матеріалами конференції [10].

DOI 10.36074/logos-16.09.2022.23

МОДЕЛИРОВАНИЕ АТАКИ СТЕГАНОКОНТЕНТА ПРИ ГРУБЫХ ОЦЕНКАХ ПОДОБИЯ ИСХОДНЫХ ДАННЫХ И РАЗНОЙ БАЗЕ СТЕКА ВЫБОРКИ СЕРИЙ

ORCID ID: 0000-0002-9790-7260 **Гончаров Никита Александрович**
студент магистратуры факультета компьютерных наук
Харьковский национальный университет имени В. Н. Каразина

Лесная Юлия Евгеньевна
студентка магистратуры факультета компьютерных наук
Харьковский национальный университет имени В. Н. Каразина

НАУЧНЫЙ РУКОВОДИТЕЛЬ:

ORCID ID: 0000-0001-8826-1616 **Малахов Сергей Витальевич**
канд. техн. наук, старший научный сотрудник,
доцент кафедры безопасности информационных систем и технологий
Харьковский национальный университет имени В. Н. Каразина

УКРАИНА

Представлены результаты моделирования попыток неавторизованного извлечения/атаки стеганоконтента (*полутоновых изображений*), защищаемого посредством реализации межблочного мультиплексирования действующих параметров массива длин серий, с использованием короткого и широкого стека выборки (*т.е. с разной базой перестановок*) серий опорных блоков [1-4].

В ходе моделирования использовался первый вариант предобработки исходных данных [1], с размером матрицы окна сглаживания 3×3 эл. и последующим формированием базового массива серий опорных блоков (ОБ) размерностью 4×4 эл. Результаты попыток нелегитимного извлечения контента представленные на рис.1, характерны для случая использования ***короткого*** стека выборки мультиплексируемых параметров, схема работы которого представлена в работе [3]. Следует отметить, что в данном цикле экспериментов проводилось одновременное мультиплексирование сразу обоих параметров (*самого ОБ и длины*) базового массива серий ОБ, как для широкого, так и короткого стеков выборки серий (*см. рис.2*). Кроме того, главной отличительной особенностью представленных на рис.1 результатов является, «грубая реализация» процедуры предобработки (*сглаживания*) исходных данных. В контексте данного материала, под термином ***«грубая реализация»*** процедуры сглаживания, следует понимать намеренное использование завышенных значений порога заметности искажений «*Pz*», причем сразу на двух этапах работы алгоритма [1]: - этапе предобработки (*сглаживания*) входных данных; - этапе формирования массива серий ОБ.

Использование критичных параметров обработки исходных данных исключает разумный компромисс между статистическими особенностями тестовых изображений (*см. рис.1(e)*) и особенностями зрительной системы человека [5-6]. Однако, использование намеренно завышенных значений «*Pz*», *последовательно* на 2-х этапах обработки, позволяет проявить основные эффекты, проявляющиеся вследствие использования критичных параметров настроек исследуемого прототипа стеганоалгоритма, с одной стороны, и отобразить динамику изменения характерных артефактов (*являющихся*

Рисунок А.24 — Перша сторінка доповіді [10], с.86.

Сертифікат

учасника III заочно міжнародної науково-практичної конференції

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

Grail of Science
Periodical scientific journal
№ 17 July 2022

INDEX COPERNICUS INTERNATIONAL

Certificate of state registration of the print media: KB24638-14578ПР issued by the Ministry of Justice of Ukraine on 04.12.2020

DOI 10.36074/grail-of-science.22.07.2022

OUCI Crossref ORCID ResearchGate

EUROPEAN SCIENTIFIC PLATFORM ICCM

GS 220722-071
dated 22.07.2022

CERTIFICATE OF PARTICIPATION AND PUBLICATION

Certificate provides at least a 0,3 ECTS credits to awarded participants for being involved.

Mykyta Honcharov

participated in the III Correspondence International Scientific and Practical Conference
SCIENCE OF POST-INDUSTRIAL SOCIETY:
GLOBALIZATION AND TRANSFORMATION PROCESSES

held on July 22th, 2022 by | NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

and published scientific paper

АДАПТАЦИЯ ПРИНЦИПА КОДИРОВАНИЯ ДЛИН СЕРИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ ПОПЫТКАМ НЕАВТОРИЗОВАННОЙ ЭКСТРАКЦИИ СТЕГАНОКОНТЕНТА

Euro Science Certificate № 22378 dated 12.06.2022 ISSN 2710-3056 DOI 10.36074/grail-of-science.22.07.2022

Head of the European Scientific Platform
Chairman of the Organizing committee
HOLDENBLAT MARIIA

Head of Community Outreach
LLC «International Centre Corporative Management»
RACHAEL APARO

Рисунок А.25 – Сертифікат участника (публікації) конференції [11].

III Заочна Міжнародна науково-практична конференція

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

Рисунок А.26 – Обкладинка збірника статей з матеріалами конференції [11].

Міжнародний науковий журнал «Грааль науки» | № 17 (липень, 2022)

241

ARTICLE

DOI 10.36074/grail-of-science.22.07.2022.042

АДАПТАЦИЯ ПРИНЦИПА КОДИРОВАНИЯ ДЛИН СЕРИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ ПОПЫТКАМ НЕАВТОРИЗОВАННОЙ ЭКСТРАКЦИИ СТЕГАНОКОНТЕНТА

Гончаров Никита Александрович
студент факультета компьютерных наук (магистрант)
Харьковский национальный университет имени В.Н. Каразина, Украина

Лесная Юлия Евгеньевна
студентка факультета компьютерных наук (бакалавр)
Харьковский национальный университет имени В.Н. Каразина, Украина

Малахов Сергей Витальевич
канд. техн. наук, ст. науч. сотрудник, доцент кафедры безопасности информационных систем и технологий
Харьковский национальный университет имени В.Н. Каразина, Украина

Аннотация: *Рассмотрена возможность использования принципа кодирования длин серий, для обеспечения межблочного мультиплекса данных гибридного стеганоалгоритма. Отмечена ведущая роль параметра длины серий в рамках процедуры противодействия нелегитимной экстракции видеоданных. Представлена взаимосвязь параметров обработки изображений с количеством серий и комбинаторикой используемых ключевых элементов*

Ключевые слова: *кодирование длин серий; стеганография; контент; взлом; стек.*

Введение. Специалистам в области обработки изображений хорошо известен метод кодирования длин серий, который отличается простотой реализации и имеет малую вычислительную сложность. Его использование в системах сжатия видеоданных и форматах представления графической информации, позволяет получить хорошие результаты при обработке изображений имеющих ограниченную цветовую или яркостную палитру (*полутоновые изображения*), и/или содержащие протяженные фоновые области с более-менее однородной заливкой [1-4].

Учитывая специфику зрительной системы человека и особенности

Рисунок А.27 — Перша сторінка доповіді [11], с.241.

Сертифікат

учасника IV заочної міжнародної науково-практичної конференції

AN INTEGRATED APPROACH TO SCIENCE MODERNIZATION: METHODS, MODELS AND MULTIDISCIPLINARITY

Рисунок А.28 – Сертифікат участника (публікації) конференції [12].

IV Заочна Міжнародна науково-практична конференція

AN INTEGRATED APPROACH TO SCIENCE MODERNIZATION: METHODS, MODELS AND MULTIDISCIPLINARITY

Рисунок А.29 – Обкладинка збірника статей з матеріалами конференції [12].

Міжнародний науковий журнал «Грааль науки» | № 18-19 (серпень, 2022)

ARTICLE

DOI 10.36074/grail-of-science.26.08.2022.31

МОДЕЛЮВАННЯ СПРОБ ЕКСТРАКЦІЇ СТЕГАНОКОНТЕНТА ПРИ РІЗНІЙ ДОВЖИНІ СТЕКУ ВИБІРКИ ПАРАМЕТРІВ СЕРІЙ

Гончаров Микита Олександрович
студент факультету комп'ютерних наук (*магістрант*)
Харківський національний університет імені В.Н. Каразіна, УКРАЇНА

Лєсная Юлія Євгеніївна
студентка факультету комп'ютерних наук (*бакалавр*)
Харківський національний університет імені В.Н. Каразіна, УКРАЇНА

Малахов Сергій Віталійович
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, УКРАЇНА

Анотація. *Розглянуто деякі результати, які були отримані в рамках моделювання спроб несанкціонованого вилучення (атаки) стеганоконтенту, що «захищається» за допомогою впровадження механізму міжблокового мультиплексування параметрів довжин серій блоків зображень, в умовах використання стеків вибірки серій різної довжини. Наочно продемонстрований взаємозв'язок параметрів обробки контенту (напівтонових зображень) з кількістю серій і комбінаторикою складових елементів отриманих пар параметрів серій, які виступають об'єктами міжблокового мультиплексування.*
Ключові слова: *кодування довжин серій; стеганографія; контент; злом; стек.*

Вступ. Матеріал даної роботи стисло представляє результати моделювання процедур з адаптації методу кодування довжин серій для забезпечення міжблокового мультиплексу даних стеганоконтента, як основного механізму протидії спробам нелегітимного вилучення даних (*у даному випадку зображення-контенту*) зі стеганоконтейнера. Дані результати експериментів є складовою частиною циклу досліджень, що проводяться в межах відпрацювання загальної концепції створення малоресурсного гібридного стеганографічного алгоритму [1-2]. Важливо підкреслити що, на даному етапі моделювання, попереднє згладжування вихідних зображень, не проводилося, що в певної мірі, дещо збільшує загальну кількість серій у вихідному (базовому) масиві зображення-контенту. Однак, у діючому прототипі дослідницького алгоритму, на етапі передобробки даних використовуються різні способи згладжування вихідних зображень, що дозволяю отримувати необхідний результат з кількості блоків ідентичного змісту при заданих критеріях візуальної помітності спотворень. В якості тестових зразків даних, були використані напівтонові зображення трьох різних типів, основна

Рисунок А.30 — Перша сторінка доповіді [12], с.173.

Сертифікат

учасника XXX міжнародної науково-практичної конференції

THE NEWEST PROBLEMS OF SCIENCE AND WAYS TO SOLVE THEM

Рисунок А.31 – Сертифікат участника (публікації) конференції [13].

XXX Міжнародна науково-практична конференція

THE NEWEST PROBLEMS OF SCIENCE AND WAYS TO SOLVE THEM

Рисунок А.32 – Обкладинка збірника статей з матеріалами конференції [13].

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ МЕЖБЛОЧНОГО МУЛЬТИПЛЕКСА ПАРАМЕТРОВ ДЛИН СЕРИЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ ПОПЫТКАМ НЕАВТОРИЗОВАННОГО ИЗВЛЕЧЕНИЯ СТЕГАНОКОНТЕНТА

Гончаров Никита Александрович
студент факультета компьютерных наук (магистрант)
Харьковский национальный университет имени В. Н. Каразина, Украина

Малахов Сергей Витальевич
канд. техн. наук, ст. науч. сотрудник, доцент кафедры
Харьковский национальный университет имени В. Н. Каразина, Украина

Представленный материал имеет целью краткое ознакомление с результатами моделирования процедур адаптации принципа кодирования длин серий [1-2] в интересах обеспечения межблочного мультиплекса данных стеганоконтента [3-4], как основного механизма противодействия попыткам нелегитимного извлечения данных (*в данном случае изображения-контента*) из контейнера. Данный цикл исследований является составной частью экспериментов, проводимых в рамках отработки общей концепции малоресурсного гибридного стеганографического алгоритма [3].

При моделировании основных процедур предобработки стеганоконтента использованы различные способы сглаживания исходных изображений, позволяющие получить требуемый результат по количеству блоков идентичного содержания [3-4] при заданных критериях визуальной заметности искажений. В качестве тестовых образцов, использованы полутоновые изображения трех типов, основное отличие между которыми заключается в характерных значениях вероятности перепада яркости между соседними элементами изображений [1, 5].

Для анализа полученных эффектов, использована упрощенная версия межблочного мультиплекса данных, ограниченная комбинаторикой только 2-х элементов (*количества ОБ и длин серий*) в общей структуре составного ключа экстрактора стеганоконтента. При этом для имитации последствий противодействия попыткам взлома контента, была реализована упрощенная версия межблочного мультиплекса данных, ограниченная стеком всего из 4-х серий опорных блоков [6]. Другими словами, предполагалось, что атакующий верно определил способ организации развертки серий [7] и действующий параметр длины стека (*базу выборки текущих параметров длин серий*) [6], однако последовательно ошибался с действующими значениями ключевых параметров: – параметра смещения опорных блоков (ОБ); – параметра длины серий ОБ. Таким образом, если даже на малой длине демонстрационного стека, получаемый эффект (*разрушение исходных данных*) будет заметен, то при

Рисунок А.33 — Перша сторінка доповіді [13], с.248.

Сертифікат

учасника II міжнародної студентської наукової конференції

КОНЦЕПТ НАУКИ XXI: СТРАТЕГІЇ, МЕТОДИ ТА НАУКОВІ ІНСТРУМЕНТИ

Рисунок А.34 – Сертифікат участника (публікації) конференції [14].

II Міжнародна студентська наукова конференція

КОНЦЕПТ НАУКИ XXI: СТРАТЕГІЇ, МЕТОДИ ТА НАУКОВІ ІНСТРУМЕНТИ

Рисунок А.35 – Обкладинка збірника статей з матеріалами конференції [14].

Гончаров Микита Олександрович, студент факультету
комп'ютерних наук (магістрант)
Харківський національний університет імені В.Н. Каразіна, Україна

Науковий керівник: Малахов Сергій Віталійович, канд. техн. наук,
доцент кафедри безпеки інформаційних систем і технологій,
старший науковий співробітник
Харківський національний університет імені В.Н. Каразіна, Україна

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ ПРОЦЕДУР БАГАТОРІВНЕВОГО МУЛЬТИПЛЕКСУ ДАНИХ ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ

Актуальність. Добре відомо, що одним із ефективних напрямів забезпечення приховування фактів передачі і зберігання інформації, є застосування різних стеганографічних методів. Принциповим є те, що в незалежності від використаного напрямку стеганографії, необхідно забезпечувати мінімізацію демаскуючих аномалій використовуваних контейнерів та підтримувати заданий рівень стійкості контенту стосовно спроб його неавторизованої екстракції, а в деяких випадках, і стійкості до спроб навмисного спотворення контейнерів.

Процес інкапсуляції в цифрові зображення (*далі - контейнери*) будь-якої іншої – корисної інформації, призводить до спотворень цих об'єктів – переносників даних. При збалансованих налаштуваннях стеганоалгоритму, можливо забезпечувати рівень спотворень зображення-контейнеру, котрі знаходяться нижче порога чутливості зорової системи людини, що забезпечує фактичну відсутність помітних аномалій контейнерів. Т.ч. забезпечується необхідний баланс між збереженням характерних властивостей для використовуваного типу зображень-контейнерів, та величиною допустимих спотворень, прийнятних для заданого типу прихованого контенту.

При цьому, слід мати на увазі, що при обробці контейнерів і контенту можуть бути використані, як однотипні (*симетричні*) режими обробки, так і режими, що реалізують різні параметри обробки даних (*асиметричні*). Такими відмінностями можуть бути: розмір блоків; параметри попередньої вихідних даних контейнерів і контенту; критерії оцінки значущої інформації контейнерів і контенту; відмінності реалізацій прискорення обчислювальних процедур та інше. Таким чином, на одних і тих же типах вихідних даних можна отримати різний ефект, з точки зору помітності артефактів, та окремих параметрів роботи самого алгоритму. Крім того для авторизованої екстракції контенту потрібна інформація, щодо параметрів багаторівневого мультиплексування даних.

Основна частина. В ході досліджень були розглянуті питання, стосовно реалізації процедур попередньої обробки і подальшої інкапсуляції контенту (*зображень*) та визначені особливості основних етапів стеганографічного алгоритму, в межах прийнятої концепції його створення [1-2].

Дослідна модифікація алгоритму забезпечує необхідне препарування і підготовку даних контейнера та контенту, з подальшим багаторівневим мультиплексом даних (*всього 3 рівні*), що формують основні позиції в структурі

Рисунок А.36 — Перша сторінка доповіді [14], с.155.

Сертифікат

учасника VI міжнародної науково-практичної конференції

MULTIDISCIPLINARY SCIENTIFIC NOTES. THEORY, HISTORY AND PRACTICE

Рисунок А.37 – Сертифікат участника (публікації) конференції [15].

VI Міжнародна науково-практична конференція

MULTIDISCIPLINARY SCIENTIFIC NOTES. THEORY, HISTORY AND PRACTICE

Рисунок А.38 – Обкладинка збірника статей з матеріалами конференції [15].

TECHNICAL SCIENCES
MULTIDISCIPLINARY SCIENTIFIC NOTES. THEORY, HISTORY AND PRACTICE

МОДЕЛЮВАННЯ КОРОТКОГО СТЕКУ ВИБІРКИ ДОВЖИН СЕРІЙ ПРИ РІЗНИХ КОМБІНАЦІЯХ ПАРАМЕТРІВ МУЛЬТИПЛЕКСУВАННЯ

Лєсная Юлія Євгеніївна
студентка факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Гончаров Микита Олександрович
студент факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Малахов Сергій Віталійович
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, Україна

У роботі представлені результати моделювання процедур атаки стеганоконтента, що протистоїть спробам його несанкціонованої екстракції з контейнера, за допомогою процедур дворівневого мультиплексування [1] параметрів серій опорних блоків (ОБ) зображення. Для демонстрації одержуваних ефектів у тестовій версії дослідницького алгоритму реалізовано вибіркове «відключення» кожного з 2-х передбачених етапів обробки контенту:

1 – процедур внутрішньоблокового мультиплексування коефіцієнтів трансформант, що характеризують середню яскравість сформованих ОБ (елементи (0;0) на рис.1 у роботі [2]), що отримані за результатами реалізації кодування з перетворенням *(у даному випадку – дискретне косинусне перетворення)* [3]. Тобто, в даному випадку, захист контенту забезпечувався реалізацією процедур виключно на рівні міжблокового мультиплексу;

2 - процедур міжблокового мультиплексування поточних параметрів довжин серій ОБ [2]. На рис.1, дана операція відповідає блоку «*Multiplex Level 1*» (крок №4). Тобто, в даному разі захист контенту обмежується реалізацією процедур внутриблочного мультиплекса.

Таким чином, на рис.1 блок «*Multiplex Level 1*» (крок №4), відповідає режиму міжблокової обробки, а блок «*Multiplex Level 2*» (крок №6), режиму внутрішньоблокового мультиплексування діючих параметрів контенту. Представлена на рис.1 схема в спрощеному вигляді пояснює основну суть процедур, які проводяться, в рамках обраної концепції моделювання. Коротко пояснимо суть проведеної обробки.

На 1-му етапі дослідницького алгоритму проводиться зчитування вихідних даних тестового зображення. На 2-му кроці реалізується процедура згладжування вихідних даних [1, 4], з використанням встановленого значення порога загрублення *(Pz)* величини яскравості сусідніх елементів оброблюваних блоків зображення.

Рисунок А.39 — Перша сторінка доповіді [15], с.684.

Сертифікат

учасника XXXVI міжнародної науково-практичної конференції

THE MAIN PROSPECTS FOR THE DEVELOPMENT OF SCIENCE IN MODERN LIFE

Рисунок А.40 – Сертифікат участника (публікації) конференції [18].

XXXVI Міжнародна науково-практична конференція

THE MAIN PROSPECTS FOR THE DEVELOPMENT OF SCIENCE IN MODERN LIFE

Рисунок А.41 – Обкладинка збірника статей з матеріалами конференції [18].

МОДЕЛИРОВАНИЕ АТАКИ СТЕГАНОКОНТЕНТА НА КОРОТКОМ СТЕКЕ ВЫБОРКИ ПАРАМЕТРОВ СЕРИЙ ПРИ ГРУБЫХ ОЦЕНКАХ ПОДОБИЯ ИСХОДНЫХ ДАННЫХ

Гончаров Никита Александрович
студент факультета компьютерных наук (магистрант)
Харьковский национальный университет имени В. Н. Каразина, Украина

Лесная Юлия Евгеньевна
студентка факультета компьютерных наук (бакалавр)
Харьковский национальный университет имени В. Н. Каразина, Украина

Семёнов Артём Сергеевич
студент факультета радиоэлектроники, компьютерных систем и инфокоммуникаций (бакалавриат)
Национальный аэрокосмический университет им. М.Е. Жуковского, "ХАИ", Украина

Малахов Сергей Витальевич
канд. техн. наук, ст. науч. сотрудник, доцент кафедры
Харьковский национальный университет имени В. Н. Каразина, Украина

Рассмотрены результаты моделирования попыток неавторизованного извлечения стеганоконтента (*полутоновых изображений*), защищаемого посредством реализации межблочного мультиплексирования действующих параметров массива длин серий [1-2] с использованием короткого стека выборки (*т.е. узкой базы перестановок*) серий опорных блоков [3-4].

В ходе моделирования использовался первый вариант предобработки исходных данных [1], с размером матрицы окна сглаживания 3×3 эл. и последующим формированием базового массива серий опорных блоков (ОБ) размерностью 4×4 эл. Для противодействия попыткам нелегитимного извлечения контента, в данном случае, использовался ***короткий стек*** выборки мультиплексируемых параметров, схема работы которого представлен на рис.1 в работе [3]. Следует отметить, что в данном цикле экспериментов проводилось мультиплексирование сразу 2-х параметров базового массива серий ОБ, т.е. самих ОБ и количества его повторений *(параметра длины)*. Кроме того, главной отличительной особенностью представленных ниже результатов является, «грубая реализация» процедуры предобработки (*сглаживания*) исходных данных. В контексте данного материала, под термином ***«грубая реализация»*** процедуры сглаживания, следует понимать намеренное использование завышенных значений порога заметности искажений «*Pz*», причем сразу на двух

Рисунок А.42 — Перша сторінка доповіді [18], с.344.

КОМП’ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

COMPUTER SCIENCE AND CYBERSECURITY (CS&CS)

Рисунок А.43 - Обкладинка журналу [24].

ISSN 2519-2310 CS&CS, Issue 1(21) 2022

УДК 621.327:621.391

ВИКОРИСТАННЯ ПАРАМЕТРІВ ДОВЖИН СЕРІЙ, ЯК ЕЛЕМЕНТА МІЖБЛОЧНОГО МУЛЬТИПЛЕКСУ ДАНИХ СТЕГАНОАЛГОРИТМУ

Микита Гончаров, Юлія Лєсная

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
worldxdark@gmail.com, xa12284109@student.karazin.ua

Рецензент: Володимир Хома, д.т.н., проф., Опольський політехнічний Університет, Ополе, Польща
xoma@wp.pl

Надійшла: Липень 2022.

Анотація: *Розглянуто особливості використання параметрів довжин серій та кількості сформованих опорних блоків, як елементів комплексного ключа екстрактора даних, гібридного стеганоалгоритму. Наведено результати атаки (злому) тестових зображень, які отримані для стеків вибірки різної довжини (різної бази перестановок діючих параметрів серій). Зроблено висновок про провідну роль параметра «довжина серій» при реалізації процедур міжблокового мультиплексування стеганоконтента. Наголошено, що одночасне використання дворівневого мультиплексу даних, значно розширює можливості протистояння спробам атак контенту. Встановлено, що застосування блоків з більшою розмірністю, істотно зменшує роль параметра «довжин серій», як основного елемента для руйнування структури вихідних зображень. Констатується, що збільшення довжини стека вибірки серій, розширює потенційну комбінаторику мультиплексування для діючих пар параметрів серій, та в більшої мірі руйнує кореляційні зв'язки елементів вихідного масиву даних. За результатами моделювання зроблено висновок, що використання різних способів розгортки серій забезпечує ще одну позицію в структурі ключа екстрактора даних.*

Ключові слова: *зображення; стеганографія; контейнер; контент; згладжування зображень; візуальна помітність викривлень; кодування серій; мультиплексування.*

1. Вступ

Ця робота відображає деякі результати, отримані в ході проведення моделювання основних процедур міжблокового мультиплексування даних, у рамках відпрацювання загальної концепції малоресурсного гібридного стеганографічного алгоритму [1]. На даному етапі робіт основна увага приділена дослідженню одержуваних ефектів, при використанні в якості елементів мультиплексування, діючих параметрів масиву серій [2]: – кількості опорних блоків (ОБ) зображень та параметра довжин серій ОБ. Можливість формування базового масиву серій ОБ певною мірою, забезпечується за рахунок проведення відповідних процедур «згладжування» зображень (*або передобробки вихідних даних*), що реалізованих на першому етапі роботи дослідного алгоритму [1]. У рамках моделювання процедур першого етапу було досліджено три варіанта згладжування вихідних зображень [1], які дозволяють отримати необхідний результат [2] за кількістю блоків ідентичного змісту (*тобто серій ОБ*) для різних типів вихідних даних *(у даному випадку, тестових зображень).*

В якості тестових зразків даних використані напівтонові зображення трьох різних типів: - зображення типу *«портрет»*; - зображення типу *«пейзаж»* та зображення типу *«мнемосхема»*. Основна відмінність між ними полягає в характерних значеннях ймовірності перепаду яскравості між сусідніми елементами (пікселями) зображень кожного типу [3-5].

2. Основна частина

Для демонстрації отриманих ефектів, використана *полегшена* версія дослідного алгоритму, що передбачає підтримку виключно міжблокового рівня мультиплексу діючих параметрів масиву довжин серій (*ОБ та їх довжин серій)*, який було сформовано за результатами етапу згладжування тестових зображень. Маска перестановок, котра використовується для цих параметрів, визначається відповідною позицією елемента в структурі композиційного

Рисунок А.44 — Перша сторінка статті [24], с. 30.

Сертифікат

учасника XXXIII міжнародної науково-практичної конференції

TRENDS IN THE DEVELOPMENT OF SCIENCE IN THE MODERN WORLD

Рисунок А.45 — Сертифікат за участь у роботі конференції [25].

XXXIII Міжнародна науково-практична конференція

TRENDS IN THE DEVELOPMENT OF SCIENCE IN THE MODERN WORLD

Рисунок А.46 — Обкладинка збірника статей за матеріалами конференції [25].

РЕЗУЛЬТАТЫ НЕАВТОРИЗОВАННОГО ИЗВЛЕЧЕНИЯ СТЕГАНОКОНТЕНТА ПРИ РАЗНОЙ ДЛИНЕ СТЕКА ВЫБОРКИ ДЛИН СЕРИЙ

Гончаров Никита Александрович
студент факультета компьютерных наук (магистрант)
Харьковский национальный университет имени В. Н. Каразина, Украина

Лесная Юлия Евгеньевна
студентка факультета компьютерных наук (бакалавр)
Харьковский национальный университет имени В. Н. Каразина, Украина

Малахов Сергей Витальевич
канд. техн. наук, ст. науч. сотрудник, доцент кафедры
Харьковский национальный университет имени В. Н. Каразина, Украина

В данном материале представлены результаты, полученные в ходе моделирования попыток несанкционированного извлечения стеганоконтента (*тестового полутонового изображения*), «защищаемого» посредством межблочного мультиплексирования параметров длин серий опорных блоков изображений, при использовании стека выборки серий с разной размерностью [1-5]. В первом случае использовался стек длиной в 4 серии, что обуславливало малую базу взаимных перестановок параметров серий [1,3]. Во втором случае, длина стека равнялась общему количеству сформированных серий опорных блоков (ОБ), а взаимный мультиплекс текущих параметров серий осуществлялся, как между двумя его полустеками, так и в рамках каждого из них. В обоих случаях производилось «разрушение» исходных связанных пар действующих параметров серий: ОБ + длина серии [4].

Следует обратить внимание, что в данном случае представлены результаты неудачной атаки контента (*неавторизованного извлечения тестового изображения*) при использовании развертки серий по столбцам (*слева-на право*). Под термином «развертка», в данном случае, следует понимать реализуемые способ обхода и последующий порядок выборки текущих параметров серий ОБ изображения из исходного, базового массива серий изображения-контента. При этом предполагалось, что атакующий смог определить используемый размер ОБ и действующий механизм развертки, однако допустил ошибку в параметрах действующей маски межблочного мультиплексирования для обоих параметров серий [1-3], что хорошо видно по вертикальным «дорожкам» блоков изображений извлеченного контента в фоновых областях тестового изображения на рис.1-2.

Рисунок А.47 — Перша сторінка доповіді [25], с.391.

ДОДАТОК Б

Результати моделювання процедур 1-го етапу *(згладжування)*.

(p - імовірність перепаду яскравості)

Рисунок Б.1 – Вихідне зображення типу *«Портрет»*

Рисунок Б.2 – Вихідне зображення типу *«Пейзаж»*

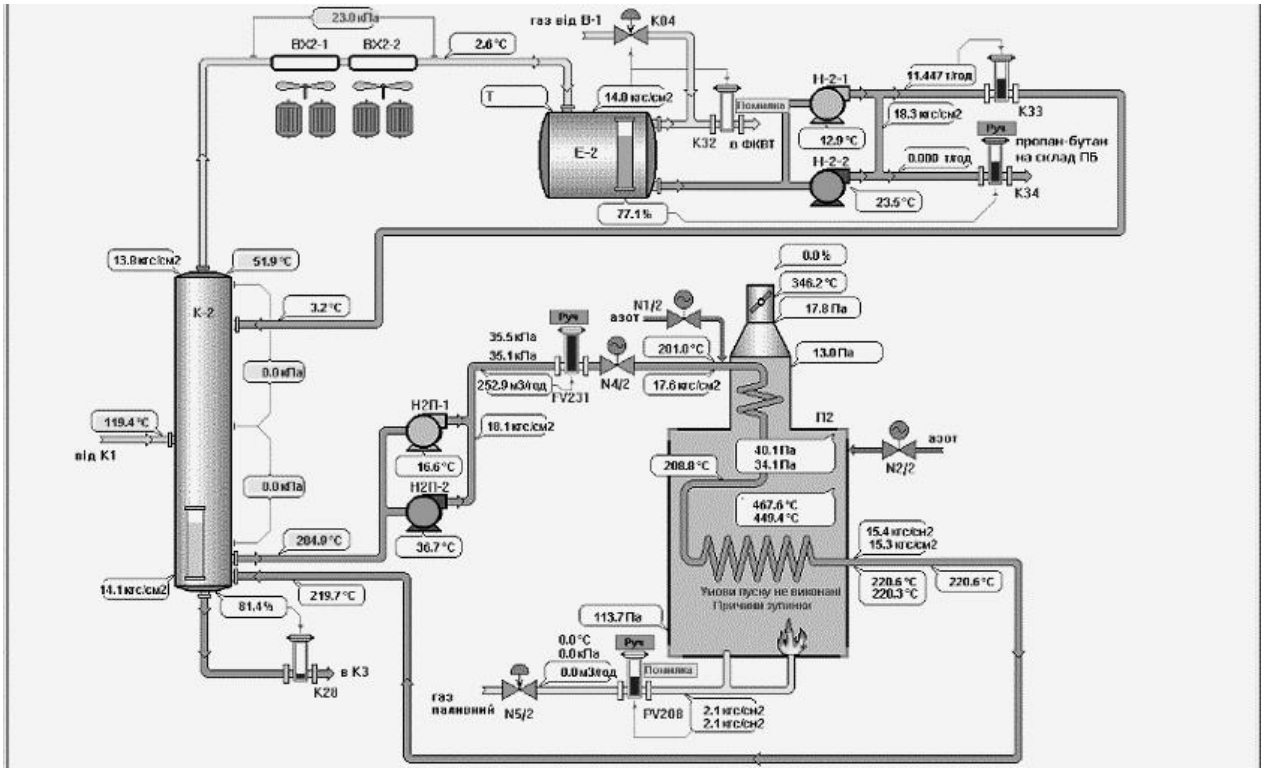


Рисунок Б.3 – Вихідне зображення типу *«Мнемосхема»*

Рисунок Б.4 – Перший варіант обробки
(маска 5×5; P_Z =7; СКП = 6.605; PSNR = 39.932; p = 0.04)

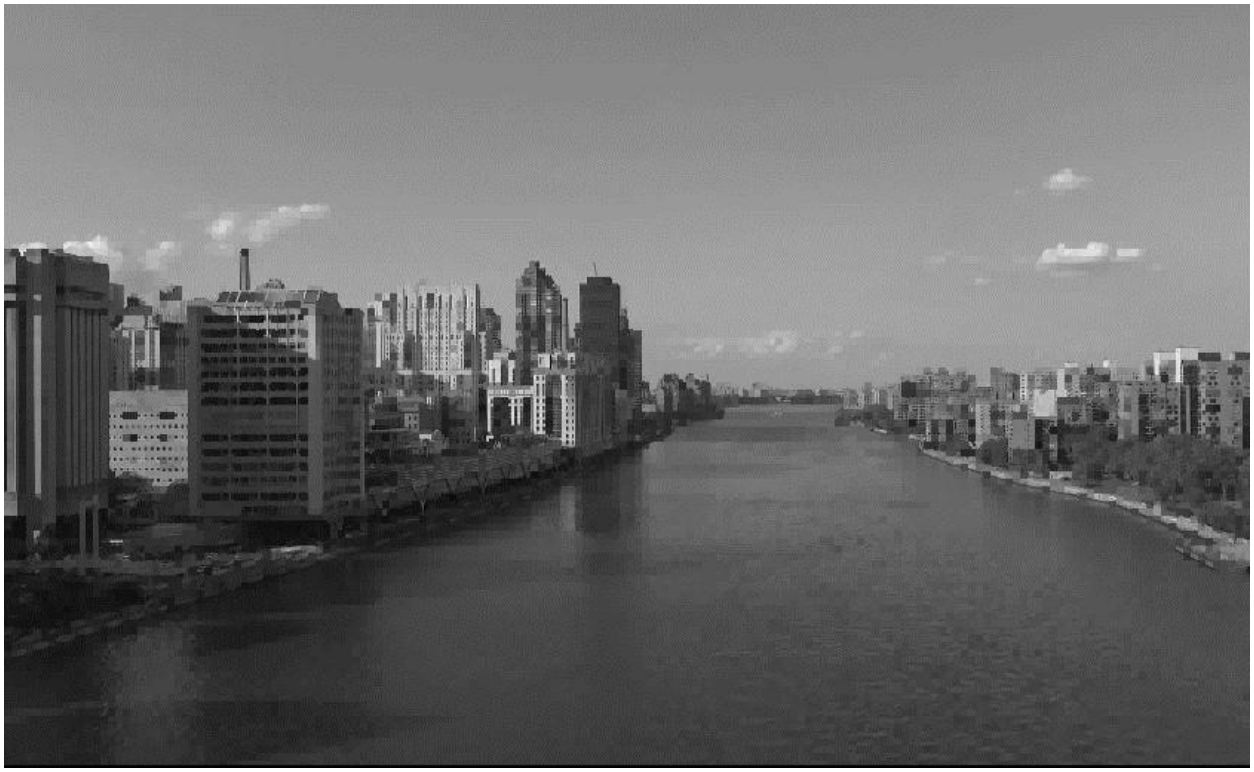


Рисунок Б.5 – Перший варіант обробки
(маска 5×5; P_Z = 7; СКП = 11.46; PSNR = 37.539; p = 0.039)

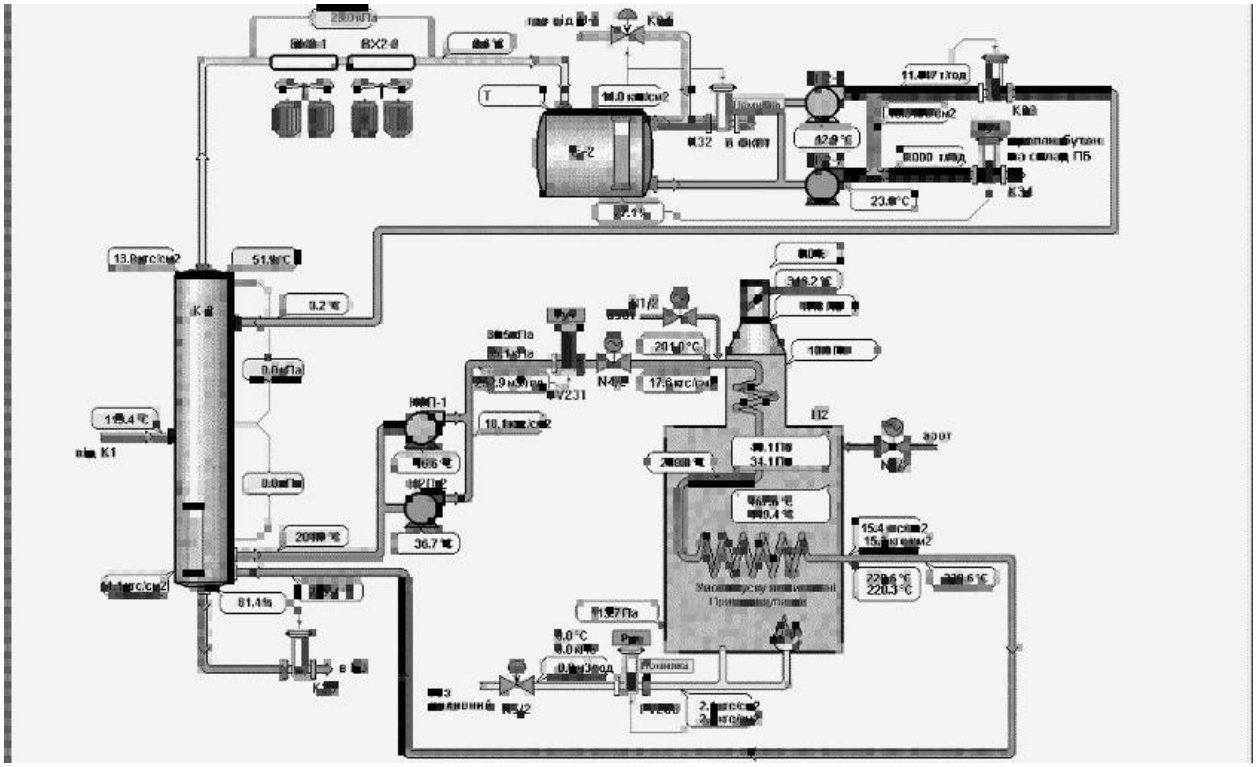


Рисунок Б.6 – Перший варіант обробки
(маска 5×5; P_Z = 7; СКП = 34.985; PSNR = 32.692; p = 0.015)

Рисунок Б.7 – Другий варіант обробки
(маска 5×5; P_Z =7; СКП = 6.572; PSNR = 39.954; p = 0.04)

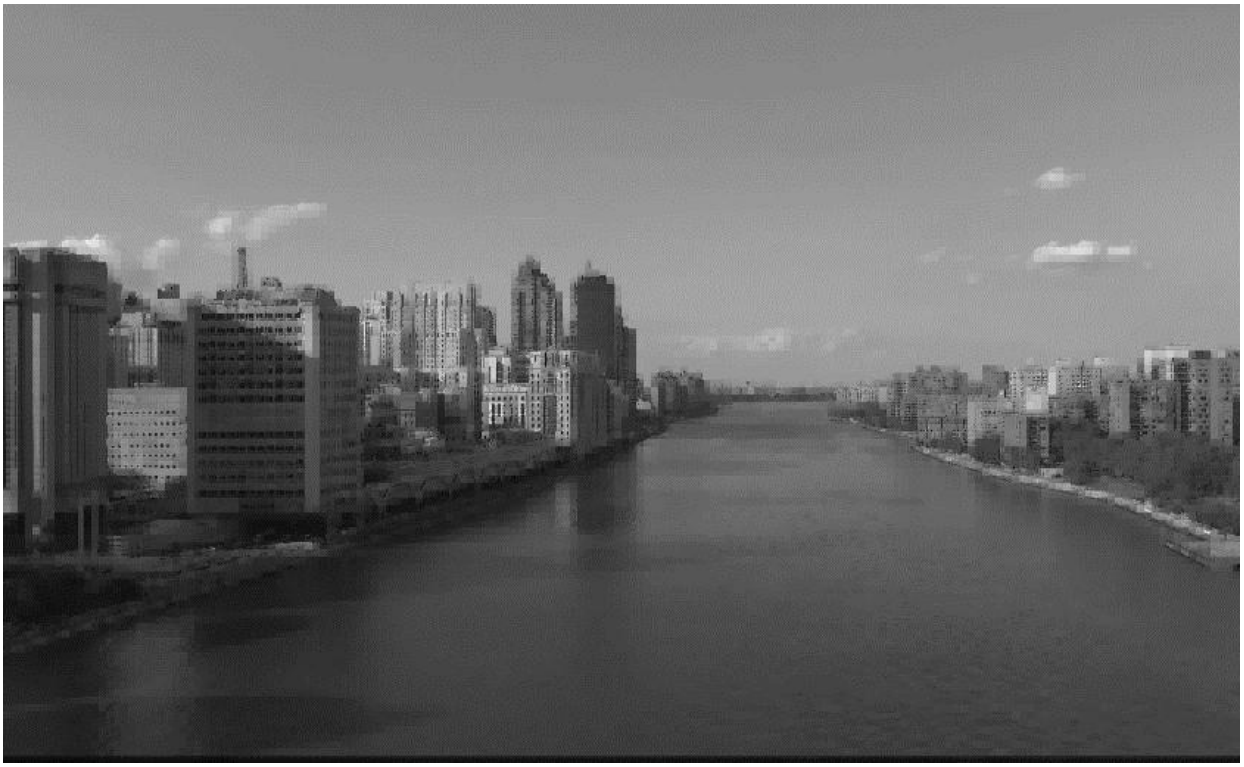


Рисунок Б.8 – Другий варіант обробки
(*маска 5×5; P_Z = 7; СКП = 10.629; PSNR = 37.866; p = 0.039*)

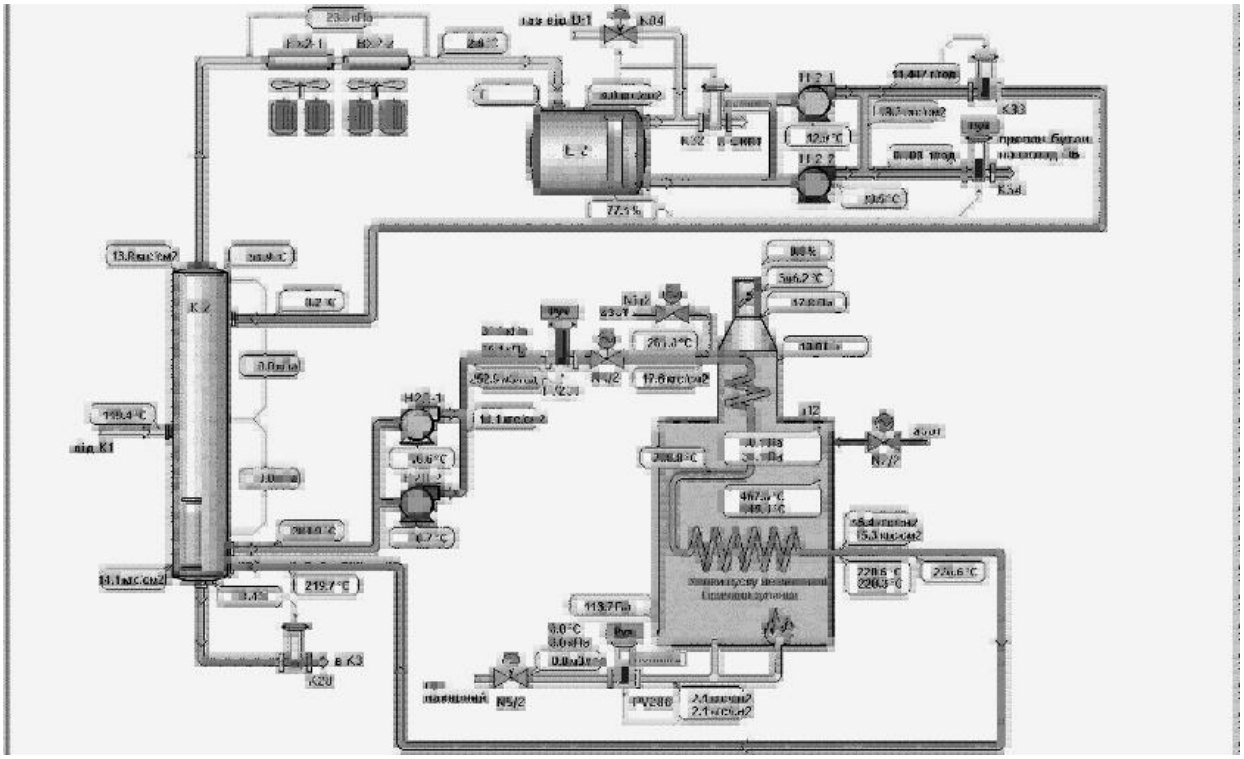


Рисунок Б.9 – Другий варіант обробки
(маска 5×5; P_Z = 7; СКП = 29.856; PSNR = 33.38; p = 0.015)

Рисунок Б.10 – Третій варіант обробки
(маска 5×5; P_Z =7; СКП = 6.069; PSNR = 40.3; p = 0.04)

Рисунок Б.11 – Третій варіант обробки
(*маска 5×5; P_Z = 7; СКП = 9.557; PSNR = 38.327; p = 0.039*)

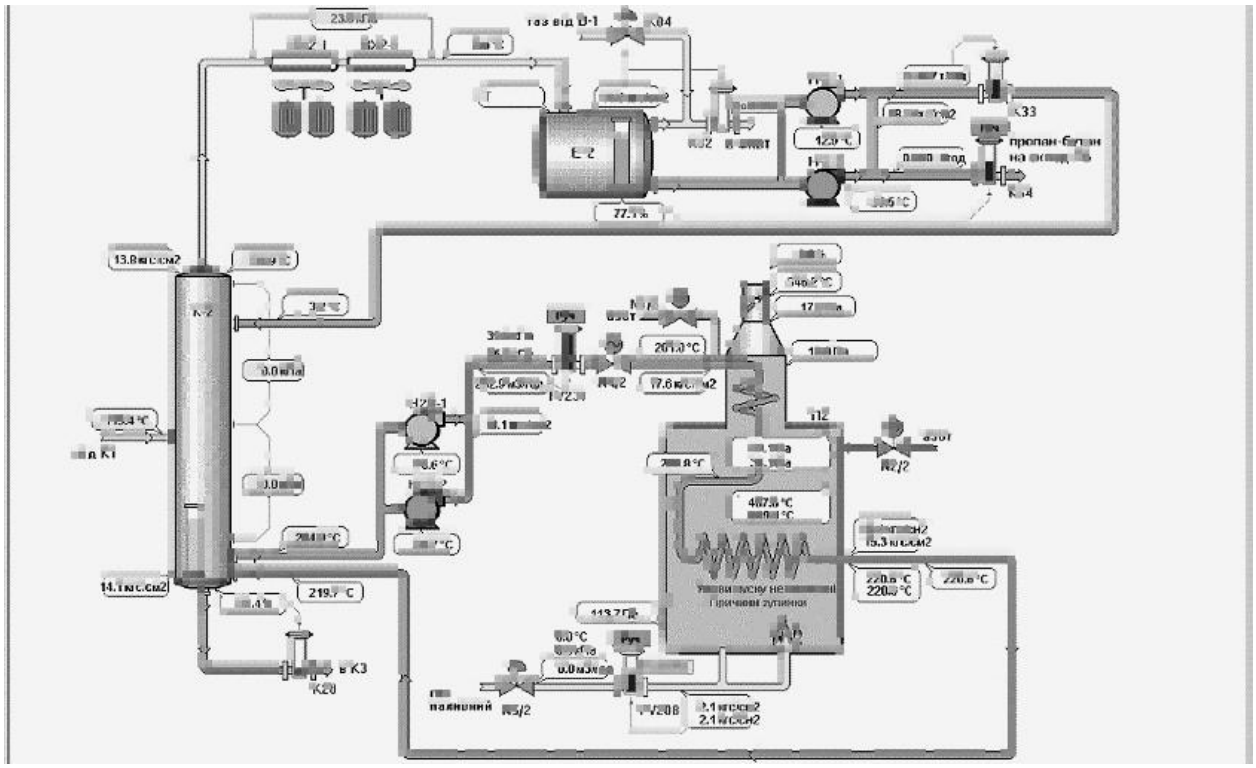
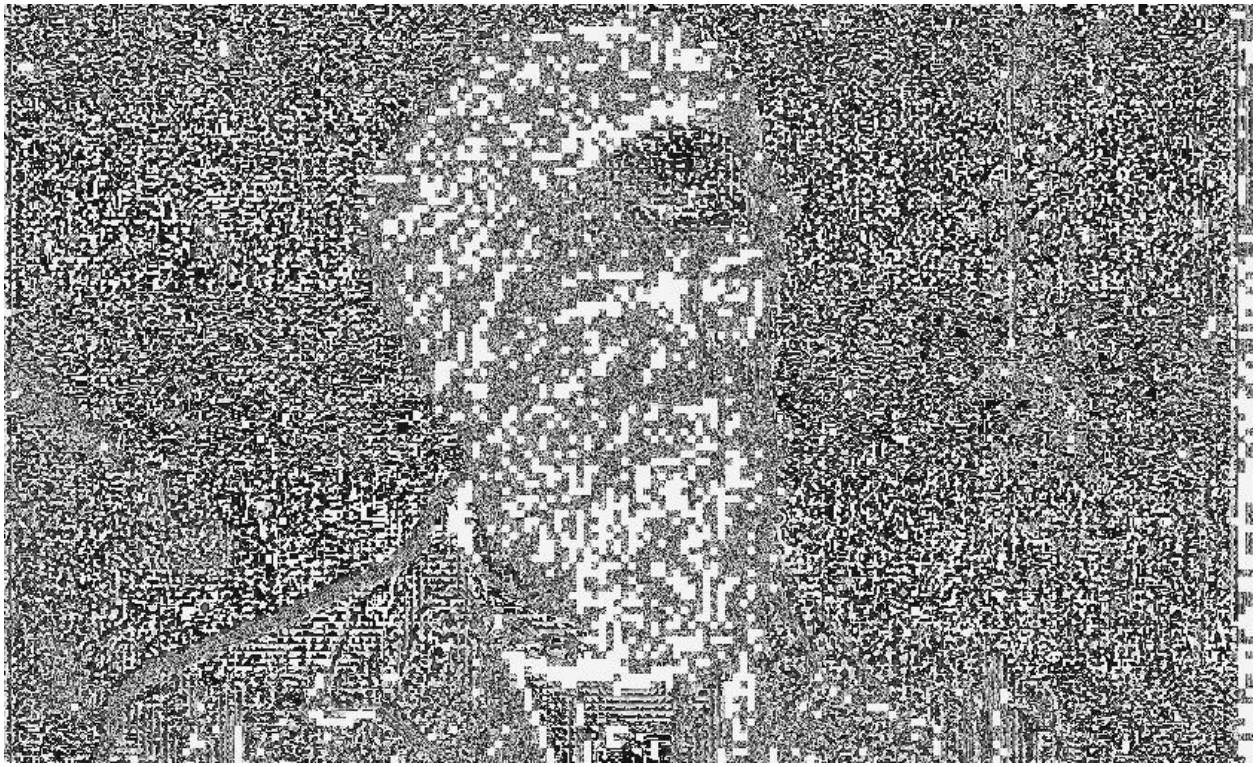
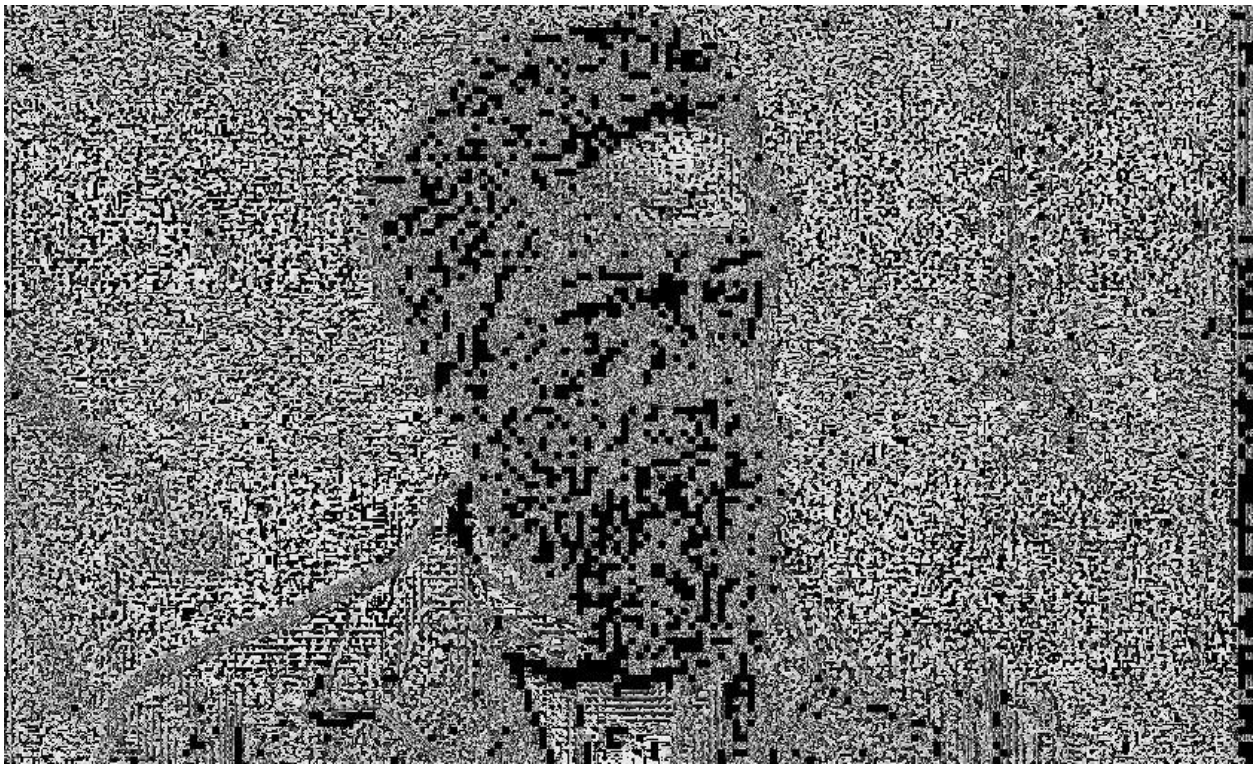


Рисунок Б.12 – Третій варіант обробки
(*маска 5×5; P_Z = 7; СКП = 24.679; PSNR = 34.207; p = 0.015*)



а)Негатив;



б) *Інверсія;*

Рисунок Б.13 – Різниця вихідного та згладженого зображень для 3-го варіанту *(маска 5×5; P_Z =7; СКП = 6.069; PSNR = 40.3; p = 0.04*)