Міністерство освіти і науки України

Харківського національного університету імені В.Н. Каразіна

Навчально-наукового інституту комп’ютерних наук та штучного інтелекту

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ

Марина ЄСІНА

«Допущено до захисту»

«  »_____2025р.

**Пояснювальна записка**

до кваліфікаційної роботи бакалавра

на тему: «Вдосконалення та дослідження програми Pixelprofile для спектрозональної розвідки щодо виявлення місць хакерської модифікації космічних та повітряних фотографій»

оцінка « _____ »

Голова ЕК

Мичуда Л.З.

Керівник: к.т.н. Громико І.О.

Рецензент: к.т.н. Шостак А.В.

Виконавець: студент групи КБ-42

Величко К.О.

Харків 2025

# РЕФЕРАТ

Пояснювальна записка до проекту бакалавра містить 51 сторінок, 19 рисунків, 1 таблицю та 41 посилань на джерела.

Мета роботи полягає в вдосконаленні програмного забезпечення PixelProfile, що призначене для автоматичного виявлення цифрових маніпуляцій із супутниковими та аерофотознімками, а також розширення функціональності програми із застосуванням нових алгоритмів спектрального аналізу.

Для досягнення поставленої мети були використані методи цифрового аналізу зображень, спектральний аналіз (2D-RGB, 3D-RGB, Фур'є-аналіз), алгоритми виявлення підробок типу Copy-Move та сплайсингу.

У результаті роботи розроблено програму PixelProfile, що дозволяє точно й ефективно виявляти цифрові модифікації супутникових та аерофотознімків без попередньо вбудованих маркерів. Головною новизною роботи є комплексне застосування спектральних, піксельних і фізичних методів, а також реалізація програмного переходу від застарілої платформи Delphi до Java.

Отримані результати рекомендовано застосовувати у сферах військової розвідки, моніторингу навколишнього середовища, геоаналітики, інформаційної безпеки та журналістських розслідувань. Програма забезпечує офлайн-середовище роботи, що є критично важливим для стратегічних і безпекових задач.

Значущість роботи полягає в тому, що розроблене програмне забезпечення дозволяє ефективно боротися з маніпуляціями цифровими зображеннями, підвищує достовірність геопросторових даних і створює умови для подальшого розвитку методів автоматизованої верифікації зображень.

Перспективи подальших досліджень полягають у впровадженні алгоритмів штучного інтелекту (CNN), автоматизації всіх етапів аналізу зображень, а також подальшому вдосконаленні методів спектрального аналізу.

Ключові слова: PIXELPROFILE, ЦИФРОВИЙ АНАЛІЗ ЗОБРАЖЕНЬ, СПЕКТРАЛЬНИЙ АНАЛІЗ, КРОСПЛАТФОРМЕННІСТЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, СУПУТНИКОВІ ЗНІМКИ, ВИЯВЛЕННЯ МАНІПУЛЯЦІЙ, COPY-MOVE.

# ABSTRACT

The explanatory note for this bachelor's project consists of 51 pages, 19 figures, 1 table, and 41 references.

The aim of this work is to improve the PixelProfile software, which is designed for the automatic detection of digital manipulations in satellite and aerial imagery. The project also focuses on enhancing the application's functionality by integrating advanced spectral analysis algorithms.

To achieve this goal, a range of image processing techniques were used, including spectral analysis methods (2D-RGB, 3D-RGB, and Fourier analysis), as well as forgery detection algorithms such as Copy-Move and splicing detection.

As a result, an upgraded version of PixelProfile was developed. It enables accurate and efficient identification of digital alterations in satellite and aerial images without the need for pre-embedded markers. The main innovation of this work lies in the combined use of spectral, pixel-level, and physical analysis methods, along with the migration of the software from the outdated Delphi platform to Java.

The results are recommended for use in military intelligence, environmental monitoring, geospatial analytics, information security, and investigative journalism. The application operates entirely offline, which is a critical feature for strategic and security-related operations.

The significance of this work is that the developed software effectively counters image manipulation, increases the reliability of geospatial data, and lays the foundation for future advancements in automated image verification technologies.

Future research directions include the implementation of artificial intelligence algorithms (e.g., convolutional neural networks), full automation of the image analysis process, and further refinement of spectral analysis methods.

Keywords: PIXELPROFILE, DIGITAL IMAGE ANALYSIS, SPECTRAL ANALYSIS, CROSS-PLATFORM, INFORMATION SECURITY, SATELLITE IMAGERY, MANIPULATION DETECTION, COPY-MOVE.

ЗМІСТ

# ПЕРЕЛІК ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АСЗ – автоматизована система зондування.

ДЗЗ – дистанційне зондування Землі.

ЗСУ – Збройні сили України.

КЗ – колірний зсув.

МЗС – маскування зон спектра.

ПП – піксельний профіль.

СЗА – спектрозональний аналіз.

ФА – Фур’є-аналіз.

ЦОІ – цифрові об’єкти інтересу.

ЧБ – чорно-білий.

AI – Artificial Intelligence (штучний інтелект).

CNN – Convolutional Neural Network (згорткова нейронна мережа).

DCT – Discrete Cosine Transform (дискретне косинусне перетворення).

ELA – Error Level Analysis (аналіз рівня помилок).

GAN – Generative Adversarial Network (генеративна змагальна мережа).

GPS – Global Positioning System (глобальна навігаційна система).

HSV – Hue, Saturation, Value (відтінок, насиченість, значення).

JPEG – Joint Photographic Experts Group (стандарт стискання зображень).

LSB – Least Significant Bit (найменш значущий біт).

RGB – Red, Green, Blue (червоний, зелений, синій).

SIFT – Scale-Invariant Feature Transform (масштабно-інваріантне перетворення ознак).

# ВСТУП

Редагування зображень є дуже серйозною проблемою в сучасному цифровому середовищі, яка безпосередньо впливає на достовірність інформації. Обробка знімків буває корисною, скажімо, для підвищення якості або виправлення кольорів. Проте часто ці інструменти використовують і не за призначенням – для фейків чи маніпуляцій.

Особливо небезпечними стають випадки, коли хакери змінюють супутникові та аерофотознімки, що може мати згубні наслідки для наукових досліджень, військової розвідки, безпеки та моніторингу навколишнього середовища. Виявлення цих змін має важливе значення для збереження безпеки і цілісності даних [1].

Цифрові технології дозволяють маніпулювати зображеннями на різних рівнях, десь це просте видалення або додавання об'єктів, а десь складні алгоритмічні методи зміни спектральних характеристик. Наприклад, під час вивчення окремих регіонів за допомогою сервісу Google Earth мною були зафіксовані випадки, коли військові об'єкти були змінені або приховані на супутникових знімках, створюючи видимість відсутньої інфраструктури або природного покриву.

До основних методів цифрової модифікації зображень належать:

- Заміна пікселів - зміна окремих пікселів для приховування певних деталей.
- Алгоритми, які використовуються у фільтрації та ретуші, щоб зробити переходи між зміненими та оригінальними областями більш плавними.
- Модифікація колірних каналів для надання зображенню природного вигляду.
- Глибокі нейронні мережі також часто використовуються для створення реалістичних підробок, які важко відрізнити від оригіналу, за допомогою штучного інтелекту [2].

Аналіз модифікованих супутникових знімків показує, що спотворення даних найчастіше трапляються у критично важливих районах, де можуть бути присутніми військові або стратегічні об'єкти. Це також підкреслює необхідність створення

автоматизованих методів аналізу, які можуть швидко і точно ідентифікувати спотворені ділянки на знімках.

Автоматичний аналіз зображень сьогодні виходить на перший план, особливо коли мова йде про дистанційне зондування Землі чи роботу з супутниковими даними. Зі збільшенням кількості супутників та зростанням роздільної здатності знімків, обсяг інформації, яку треба обробляти, зріс у рази. Якщо раніше основна частина роботи лягала на плечі експертів, які вручну переглядали і порівнювали зображення, то зараз такий підхід втрачає свою ефективність – це займає надто багато часу і не підходить для роботи з масивними архівами [3].

Верифікація зображень стає можливою здебільшого завдяки автоматизованим методам, таким як спектральний аналіз, що дозволяє виявити нерівності, які можуть вказувати на спотворення даних. Одним з інструментів, що дозволяє виявити варіації спектрального складу пікселів, які можуть вказувати на можливі маніпуляції зі структурою зображення, є програмне забезпечення PixelProfile, яке було модифіковано мною в рамках цього проекту.

Основні аспекти автоматизованого аналізу супутникових та повітряних знімків:

- Виявлення можливих підробок шляхом дослідження варіацій у колірному спектрі.
- Використання перетворення Фур'є для виявлення розбіжностей у спектральному складі різних ділянок.
- Тривимірні профілі розподілу кольорів.
- Одним із методів виявлення прихованих артефактів редагування на цифрових фотографіях є логарифмічне масштабування рівнів інтенсивності.

Адаптація програми PixelProfile до платформи Java має на меті покращити функціональність програми, сприяти кращій інтеграції з сучасними технологіями аналізу зображень та підвищити доступність програмного забезпечення для різноманітних прикладних задач. Крос-платформенна сумісність, оптимізація продуктивності та покращення зручності користувацького інтерфейсу стали

можливими завдяки переходу на Java, і ці переваги є важливими для подальшого зростання використання програми.

Дослідження має на меті провести ретельне вивчення методів дослідження кольорової структури цифрових зображень з метою вдосконалення програми, призначеної для автоматичної ідентифікації змін і можливих підробок на супутникових і аерофотознімках. Особлива увага приділяється спектральному аналізу та методам оцінки спектральних властивостей зображення, які можуть бути використані для виявлення областей з потенційними змінами або незвичайними колірними профілями.

Важливою частиною проекту є порівняння оновленого PixelProfile з існуючими програмами та методами аналізу зображень. Це дозволить оцінити ефективність розроблених мною алгоритмів та виявити їхні переваги та недоліки порівняно з альтернативними методологіями. Для забезпечення реалістичної оцінки можливостей вдосконаленого програмного забезпечення аналіз буде проводитися з використанням як тестових зображень, так і реальних супутникових або аерофотознімків.

Результати цього проекту допоможуть вдосконалити автоматизований аналіз цифрових зображень, підвищити точність ідентифікації змінених регіонів і розширити можливості використання PixelProfile в ряді областей, таких як моніторинг змін навколишнього середовища, картографія, безпека і географічні інформаційні системи.

Для оцінки структури зображення, виявлення можливих слідів редагування та порівняння ефективності різних методів обробки графічної інформації в дослідженні використовуються методи цифрового аналізу зображень. Основою дослідження є вивчення колірних профілів зображень, що дає змогу виявити нерівномірність розподілу кольорів і визначити можливі області для корекції.

Крім того, проведено порівняння програмних засобів обробки та аналізу зображень. Це дає можливість оцінити ефективність розробленого підходу, виявити його переваги та окреслити потенційні напрямки подальшого вдосконалення.

# 1 АНАЛІЗ ОСНОВНИХ ДОСЛІДЖЕНЬ

Varsha Sharma, Swati Jha, Dr. Rajendra Kumar Bharti (2016), у своїй статті розглядають різні методи виявлення підробок цифрових зображень, особливу увагу приділяючи інструментам, які аналізують змінені ділянки. Особливо виділені пасивні методи, що дозволяють знаходити нерівності в текстурі та кольоровій композиції зображень, наприклад, блочне зіставлення та дискретне косинусне перетворення (DCT). У дослідженні також оцінюється, наскільки ефективно запропонований підхід працює в умовах JPEG-стиснення та наявності шуму, що позитивно впливає на точність виявлення змін. Результати показують, що більш досконалі алгоритми значно підвищують успішність виявлення маніпуляцій на цифрових фотографіях [4].

Preeti Sharma, Manoj Kumar, Hitesh Sharma (2022), у своїй статті проводять детальний аналіз різних стратегій виявлення підробки зображень, охоплюючи як класичні підходи, так і сучасні методи на основі глибокого навчання. Особливу увагу автори приділяють як активним, так і пасивним методам цифрової криміналістики, а також використанню генеративних змагальних мереж (GAN) для створення фотореалістичних підроблених зображень, які значно ускладнюють процес їх виявлення. У роботі досліджується ефективність різних алгоритмів для виявлення маніпуляцій із зображеннями, а також аналізується їхня стійкість до таких впливів, як стиснення, редагування чи додавання штучних елементів. Запропоновані підходи оцінюються за критеріями продуктивності та точності, що демонструє великий потенціал сучасних нейронних мереж у галузі цифрової криміналістики [5].

Dr Fahimeh Abedi and Professor Abbas Rajabifard (2024), у своїй статті аналізують поєднання штучного інтелекту (ШІ) та геопросторових технологій, що призвело до появи GeoAI — інноваційної сфери аналізу просторових даних. Автори показують, як GeoAI впливає на такі галузі, як оборона, охорона здоров’я, міське планування і реагування на надзвичайні ситуації, наголошуючи на його потенціалі у покращенні процесів прийняття рішень. Значна увага приділена етичним аспектам, включаючи питання безпеки даних, конфіденційності та

можливих алгоритмічних упереджень, які можуть впливати на точність аналізу. Дослідники також підкреслюють важливість розробки регуляторних механізмів для відповідального використання GeoAI та мінімізації ризиків, пов’язаних із маніпулюванням географічною інформацією [6].

Eugene T. Lin, Christine I. Podilchuk, Edward J. Delp (2000), у статті досліджуються методи застосування напівкрихких водяних знаків для виявлення змін у цифрових зображеннях. Автори розглядають переваги й недоліки як стійких, так і нестійких водяних знаків, підкреслюючи, що стійкі водяні знаки зберігаються навіть після багаторазового редагування, тоді як нестійкі можуть легко зникати після будь-яких змін. Запропонований напівкрихкий водяний знак дозволяє зберігати невеликі виправлення, водночас забезпечуючи виявлення значних змін навіть після стиснення зображення. Дослідження демонструє ефективність цього методу для виявлення незаконних змін у цифрових фотографіях, що робить його корисним інструментом для цифрової криміналістики [7].

Mohd Dilshad Ansari, S. P. Ghrera, Vipin Tyagi (2014), у своїй статті розглядають різні способи виявлення підробок цифрових зображень, з особливим акцентом на піксельні підходи, які аналізують зміни саме на рівні окремих пікселів. Особлива увага приділяється двом найпоширенішим методам підробки — копіюванню-переміщенню та склеюванню фрагментів зображень. Автори детально обговорюють використання алгоритмів на основі аналізу головних компонент (PCA), дискретного косинусного перетворення (DCT) і методів машинного навчання для ефективного виявлення змінених ділянок. У статті також наголошується на необхідності подальших досліджень для підвищення точності методів виявлення підробок у цифрових фотографіях [8].

# 2 ОГЛЯД МЕТОДІВ АНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

## 2.1 Визначення можливостей програми PixelProfile для спектрозонального аналізу.

Щоб зрозуміти принцип роботи програми PixelProfile, спочатку необхідно розібратися, як формується цифрове зображення. Фотографія – це двовимірне зображення, представлене у вигляді набору рядків: верхній рядок №1, під ним – рядок №2, далі – №3 і так до останнього рядка №N. Кожен рядок, який зчитує ПЗЗ-матриця (прилад із зарядовим зв’язком) фотокамери, має початковий та кінцевий строчні імпульси, що визначають межі зчитування.

Оскільки ПЗЗ-матриця складається з мільйонів чутливих елементів (фотодіодів або напівпровідникових мікро конденсаторів), вона реагує на світловий потік, що потрапляє через об’єктив фотокамери. Кожен елемент матриці – піксель – накопичує або генерує енергію залежно від яскравості світла в певній точці. Оскільки світловий потік складається з трьох основних кольорових компонентів (червоного, зеленого та синього), пікселі спеціалізуються на реєстрації певного.

На ПЗЗ-матриці таких пікселів мільйони. Чим вища їхня кількість та якісніший об’єктив, тим чіткіше зображення можна отримати. Як тільки завершується процес накопичення енергії у першому рядку, сигнал від останнього строчного імпульсу надходить у процесор фотокамери. Далі процесор почергово зчитує енергетичні рівні всіх пікселів рядка та передає їх у пам’ять. Після цього розпочинається процес формування зображення для наступного рядка – і так далі, поки не буде оброблено весь кадр.

Через цей механізм цифрове зображення сприймається не як аналогове (суцільне), а як дискретне (піксельне). Відтінки кольорів, які ми бачимо, є результатом змішування кольорів сусідніх пікселів, що створює суцільне зображення для людського ока (див. рис. 2.1). Мозок сприймає цей інтегральний результат як єдину картину завдяки стимуляції нейронів фотонами різних довжин хвиль.

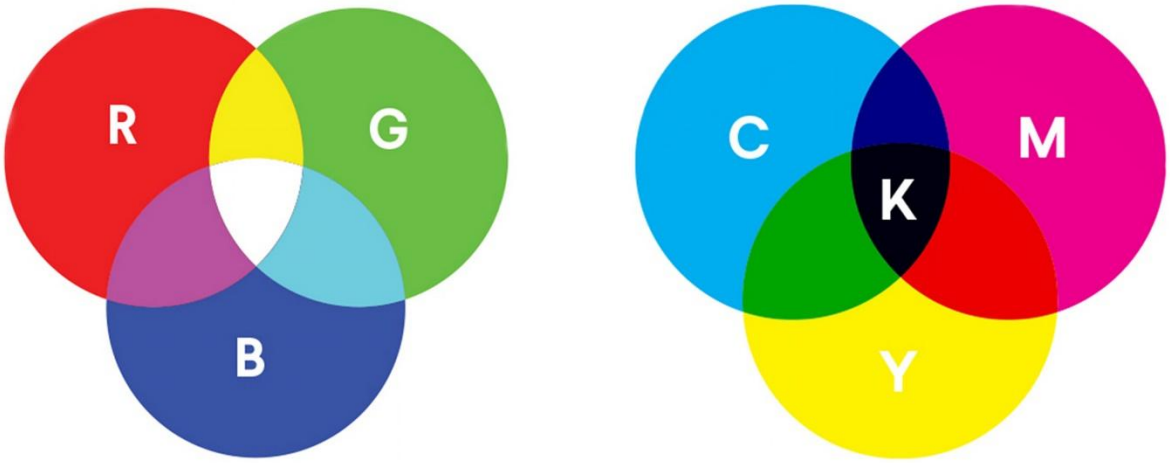



Рисунок 2.1 – Додавальне (RGB) і віднімальне (CMY) змішування кольорів [9]

Програма PixelProfile дозволяє аналізувати кількість та співвідношення червоних (R), зелених (G) і синіх (B) пікселів у кожній точці зображення. Вона може оцінювати середнє співвідношення цих компонентів у цілому кадрі та використовувати ці дані для подальшого аналізу.

Якщо програму навчити визначати середні значення співвідношення RGB-пікселів для цільного зображення, а потім подати їй інше зображення, у якому об’єкти частково накладаються на вихідне, вона може зафіксувати відмінності у співвідношенні кольорів. Проте варто враховувати, що зміни в параметрах зйомки, таких як тип об’єктива, матриці, експозиція, погодні умови та освітлення, можуть впливати на результати аналізу, що ускладнює автоматичне порівняння.

Комп’ютерна програма PixelProfile дозволяє здійснювати відображення піксельного профілю, який визначається двома точками на зображенні, показаному на екрані комп’ютера. Графік піксельного профілю можна оцінити у числових значеннях червоного, зеленого, синього кольору, а також у похідних параметрах: інтенсивності, відтінку, насиченості та цінності. Програма дає можливість переглядати піксельні дані профілю, вибравши лінію (X1, Y1; X2, Y2), щоб визначити значення R, G, B кольорового заповнення пікселів уздовж цієї лінії (див. рис. 2.2). Також можна отримати додаткові параметри: I – інтенсивність, H – відтінок, S – насиченість, V – цінність (вклад, вага, домінування тощо). Ці значення

обчислюються на основі параметрів R, G, B. Дані можна отримати у вигляді графіка для одного або трьох кольорів.

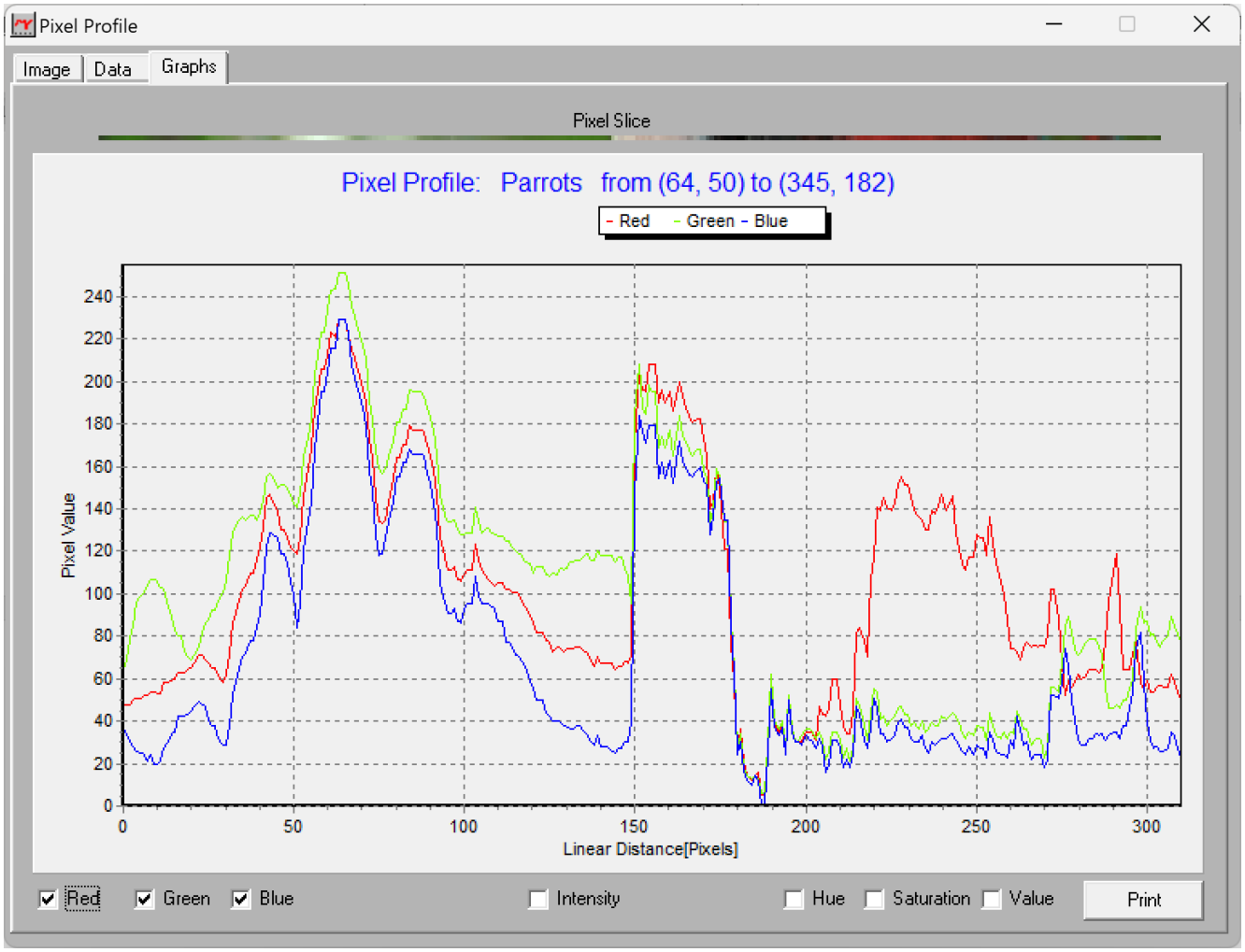



Рисунок 2.2 – Графік піксельного профілю з інтенсивностями R, G, B

Спеціальна версія для відображення зображень розміром 1024×1024 була створена на Delphi 7 (від 30 червня 2003 року). Програму перевірено за військовим стандартом США MIL-STD-150A [10]. Вихідний код програми, що демонструє приклад відображення піксельних профілів між двома довільними точками зображення, відкрито розміщено в інтернет-ресурсах. Як зазначив автор програми Earl F. Glynn, піксельний профіль може бути червоним, зеленим або синім залежно від інтенсивності кольору, насиченості та яскравості. Піксельні профілі можуть бути корисні при аналізі зображень.

Програма PixelProfile реалізує аналіз зображень у площинному (2D) режимі, що дозволяє оцінювати вибрані оператором області, а не лише окремі лінії. Наступним етапом розвитку стало вдосконалення програми для проведення

спектрозональної RGB-розвідки на основі розширеного аналізу супутникових знімків. Це включає верифікацію ділянок за допомогою GPS-координат, отриманих із відкритих картографічних сервісів, а також оцінку супутникових зображень, отриманих як з комерційних, так і з розвідувальних джерел [11]. Подальша робота спрямована на покращення алгоритмів RGB-аналізу для автоматичного виявлення змін у зображеннях. Одним із ключових завдань є розпізнавання спроб модифікації фотографій, таких як накладення "латок" для маскування техніки або інших об'єктів. Виявлення таких змін можливе завдяки аналізу спектрального складу зображення, оскільки фон вставленої області часто відрізняється від навколишнього середовища.

При накладенні одного зображення на інше зазвичай утворюється лінія стику, яку можна виявити за допомогою Фур'є-аналізу. Згідно з теорією, така лінія повинна сприйматися як одиничний короткий імпульс у просторовому оптичному аналізі. Це дозволяє скануванню виявляти зміни у текстурі або яскравості. У зв’язку з цим у програму PixelProfile був доданий Фур'є-метод аналізу зображень.

Об’ємний аналіз проводиться у будь-якому з RGB-спектрів, що дозволяє отримати тривимірне представлення аналізованої ділянки. Це дає можливість масштабувати зображення, обертати його в просторі, отримувати зрізи зображення на різних рівнях [12].

Згідно з дослідженнями у галузі радіотехніки, органи чуття людини працюють у логарифмічному масштабі. Тому в програму додано режим логарифмування яскравості зображення, що значно полегшує сприйняття інформації.

Одним із найбільш доступних методів маскування зображень є "напилення" фону на об’єкти або стики латок. Такий метод реалізований у багатьох графічних редакторах, наприклад, Adobe Photoshop або MS Paint. Програма PixelProfile-3D дозволяє виявляти такі модифікації шляхом аналізу січень зображення паралельними площинами. Це допомагає ідентифікувати момент переходу штучного фону у природне середовище.

## 2.2 Огляд сучасних методів детектування змін у цифрових фотографіях.

В сучасному цифровому світі зображення відіграють важливу роль у різних сферах життя, включаючи науку, медицину, безпеку, журналістику та соціальні мережі. З розвитком програмного забезпечення для обробки графічних даних, таких як Adobe Photoshop, GIMP, CorelDRAW, а також нейромережевих алгоритмів, стало можливим змінювати цифрові фотографії так, що навіть досвідчені експерти не завжди можуть відрізнити оригінальне зображення від підробленого. Це створює серйозні виклики для цифрової криміналістики, яка займається виявленням фактів маніпуляції та забезпеченням достовірності зображень.

Зміни у фотографіях можуть бути різного характеру – від незначного редагування (наприклад, зміна контрасту чи яскравості) до складних маніпуляцій, таких як заміна обличчя, видалення або додавання об’єктів, або створення повністю синтетичних зображень за допомогою глибоких нейронних мереж (DeepFake). Деякі з цих змін можуть мати безневинний характер, наприклад, ретуш у сфері моди чи реклами, але інші можуть використовуватися для створення фейкових новин, фабрикації доказів у судових процесах або дезінформації в політиці та військовій сфері.

Для вирішення цих проблем розроблено широкий спектр методів детектування змін у цифрових фотографіях. Вони поділяються на активні та пасивні методи. Активні методи передбачають попереднє вбудовування ідентифікаторів, таких як цифрові водяні знаки або підписи, що дозволяють перевірити оригінальність зображення. Пасивні методи, навпаки, базуються на аналізі внутрішніх статистичних, структурних та фізичних властивостей зображення без необхідності попереднього маркування [13].

Активні методи детектування змін у цифрових фотографіях передбачають попереднє вбудовування спеціальних ідентифікаторів або маркерів у зображення з метою забезпечення можливості подальшої перевірки їх автентичності та цілісності. Ці методи є ефективними для виявлення несанкціонованих змін, оскільки дозволяють точно визначити, чи було зображення піддане модифікації

після його створення. До основних активних методів належать цифрові водяні знаки та цифрові підписи.

Цифрові водяні знаки (Digital Watermarking) передбачають вбудовування прихованої інформації безпосередньо в цифрове зображення. Ця інформація може містити дані про автора, дату створення, права на використання або інші важливі відомості. Водяні знаки зазвичай є невидимими для людського ока, щоб не впливати на візуальне сприйняття зображення, але можуть бути виявлені за допомогою спеціалізованого програмного забезпечення. Існують різні техніки вбудовування водяних знаків, такі як метод найменш значущого біту (LSB), дискретне косинусне перетворення (DCT) та дискретне вейвлет-перетворення (DWT). Метод LSB полягає у заміні найменш значущих бітів пікселів зображення на біти водяного знака, що робить цей метод простим у реалізації, але менш стійким до атак. Методи DCT та DWT вбудовують водяний знак у частотну область зображення, що забезпечує вищу стійкість до різних видів обробки, таких як стиснення або фільтрація (див. рис. 2.3).

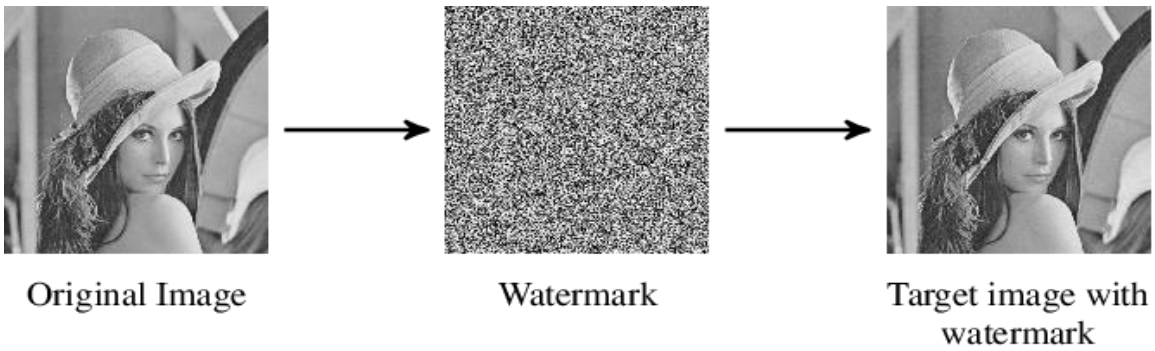



Рисунок 2.3 – Приклад вбудовування цифрового водяного знаку в зображенні [14]

Цифрові підписи (Digital Signatures) засновані на використанні криптографічних методів для забезпечення автентичності та цілісності цифрових зображень. Процес створення цифрового підпису включає обчислення хеш-значення зображення за допомогою хеш-функції, після чого це значення шифрується закритим ключем автора. Отриманий підпис зберігається разом із зображенням або в окремому файлі. Для перевірки автентичності отримувач обчислює хеш-значення отриманого зображення та розшифровує підпис за допомогою відкритого ключа автора. Якщо обидва хеш-значення співпадають, це

підтверджує, що зображення не було змінено та походить від заявленого автора. Цей метод широко використовується для захисту авторських прав та забезпечення цілісності даних у цифрових зображеннях.

Активні методи, такі як цифрові водяні знаки та цифрові підписи, є ефективними інструментами для забезпечення автентичності та цілісності цифрових зображень. Однак їх застосування вимагає попереднього вбудовування відповідних маркерів або підписів, що може бути непридатним для вже існуючих зображень або в ситуаціях, де попереднє втручання в зображення неможливе. У таких випадках доцільно використовувати пасивні методи детектування змін, які базуються на аналізі властивостей самого зображення без необхідності попереднього маркування.

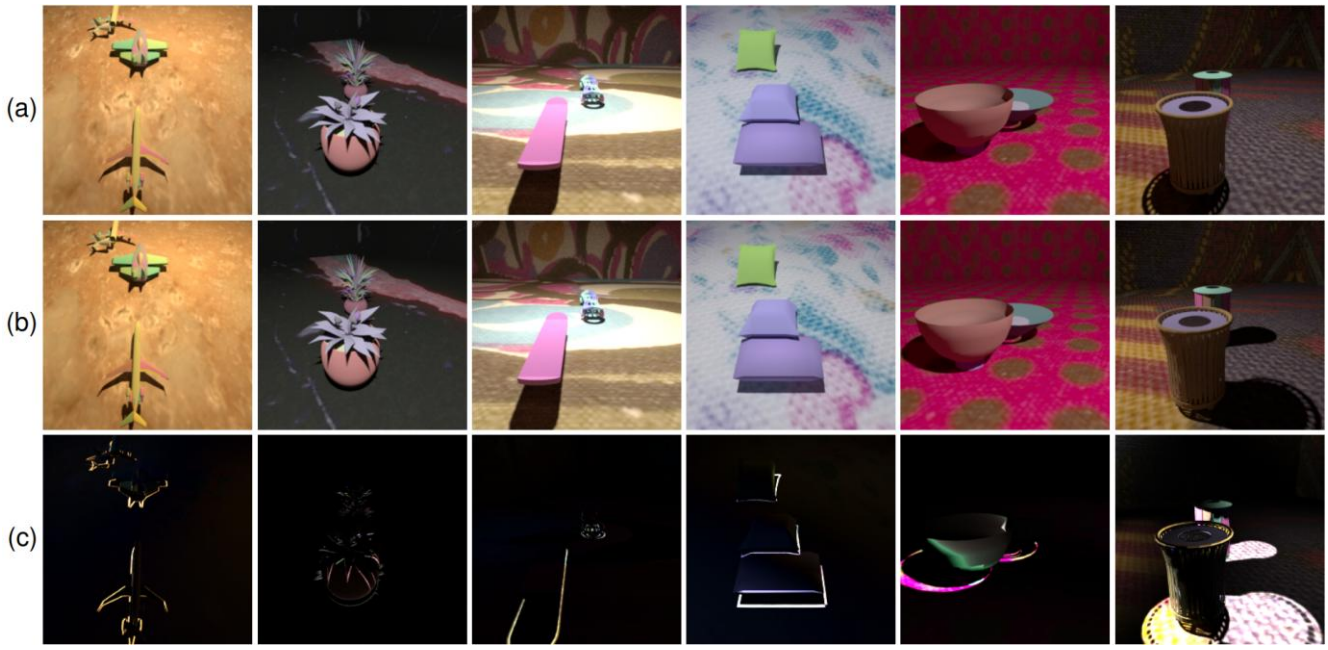
Пасивні методи детектування змін у цифрових фотографіях не потребують попереднього втручання в зображення та базуються на аналізі його статистичних, структурних або фізичних характеристик. Ці методи дозволяють виявляти маніпуляції, навіть якщо зображення не було попередньо підготовлене для перевірки автентичності.

Піксельні методи (Pixel-Based Methods) зосереджені на аналізі окремих пікселів та їхніх взаємозв'язків для виявлення аномалій. Один із поширених підходів – виявлення підробок типу "копіювання-вставка" (Copy-Move Forgery Detection), коли частина зображення копіюється та вставляється в інше місце того ж зображення (див. рис. 2.4). Для цього використовують методи, що аналізують перекриття блоків пікселів, виявляючи області з високою кореляцією. Інший підхід – аналіз артефактів стиснення JPEG (JPEG Compression Analysis), який базується на тому, що повторне стиснення зображення з різними параметрами може залишати характерні сліди, що вказують на можливі маніпуляції. Також застосовується аналіз кольорових аномалій (Color Anomaly Analysis) для виявлення невідповідностей у кольоровому профілі між різними частинами зображення, що можуть свідчити про підробку [15].

(a) (b)

Рисунок 2.4 – Приклад виявлення копіювання-вставки (Copy-Move) [16]

Фізичні методи (Physics-Based Methods) аналізують фізичні властивості сцени, відображеної на зображенні, такі як освітлення, тіні та геометрія об'єктів. Оцінка напрямку освітлення (Light Direction Estimation) передбачає перевірку відповідності напрямків освітлення та тіней на фотографії; невідповідності можуть вказувати на маніпуляції (див. рис. 2.5). Геометричний аналіз (Geometric Analysis) включає перевірку відповідності перспективи та пропорцій об'єктів на зображенні, що дозволяє виявляти вставлені або видалені елементи.




Розділ 2.5 – Оцінка освітлення: оригінал, змінене світло, різниця RGB [17]

Камерні методи (Camera-Based Methods) базуються на аналізі характеристик, притаманних конкретним моделям камер. Аналіз сенсорного шуму (Sensor Noise

Analysis) використовує унікальні шумові характеристики, властиві сенсору кожної камери, для виявлення невідповідностей, які можуть свідчити про підробку. Аналіз кольорового фільтра (Color Filter Array Analysis) перевіряє специфічні особливості кольорової фільтрації, які можуть змінюватися при маніпуляціях із зображенням. Додаткову інформацію про джерело зображення, включаючи дату зйомки, модель камери, налаштування експозиції та координати GPS, можна отримати з метаданих Exif, структура яких описана у стандарті JEITA CP-3451C. Ці дані часто використовуються у процесі цифрової криміналістики для виявлення підробок або підтвердження автентичності [18].

Методи глибокого навчання (Deep Learning-Based Methods) застосовують нейронні мережі для автоматичного виявлення маніпуляцій. Згорткові нейронні мережі (Convolutional Neural Networks, CNN) використовуються для аналізу текстур та виявлення аномалій, що можуть вказувати на підробку. Порівняння усіх методів є необхідним для розуміння поставленої задачі (див. табл. 2.1).

Таблиця 2.1 – Порівняльний аналіз детектування змін у фотографіях.

| Метод | Переваги | Недоліки |
|---|---|---|
| Digital Watermarking | Висока точність, можливість перевірки автентичності | Потребує попереднього вбудовування, вразливий до стиснення |
| Copy-Move Detection | Простий у реалізації, ефективний для локальних змін | Вразливий до геометричних трансформацій |
| JPEG Compression Analysis | Добре працює для зображень у форматі JPEG | Не працює з іншими форматами, ефективність залежить від стиснення |
| Color Anomaly Analysis | Дозволяє знаходити сплайсинг (склейку зображень) | Залежність від освітлення та якості фото |

Продовження таблиці 2.1.

| | | |
|---|---|---|
| Light Direction Estimation | Виявляє аномалії у складних маніпуляціях | Вимагає високої роздільної здатності та точного розрахунку |
| Geometric Analysis | Дозволяє виявити масштабні підробки | Вимагає точних початкових параметрів камери |
| Sensor Noise Analysis | Дозволяє визначити джерело зображення | Вимагає бази даних шумових профілів |
| Color Filter Array Analysis | Дозволяє знаходити змінені частини фото | Ефективність залежить від якості камери та освітлення |
| CNN for Texture Analysis | Автоматизований пошук аномалій, висока точність | Вимагає великих обчислювальних ресурсів та наборів даних |
| GANs for Forgery Detection | Висока ефективність у виявленні deepfake | Вразливість до контр-методів глибокого навчання |

Детектування змін у цифрових фотографіях є важливим завданням у багатьох сферах, зокрема у судовій експертизі, журналістиці, кібербезпеці та дистанційному зондуванні. Існують активні та пасивні методи перевірки автентичності зображень. Активні методи, такі як цифрові водяні знаки та підписи, є високоточними, але вимагають попередньої інтеграції механізмів захисту. Пасивні методи, навпаки, не потребують попереднього маркування, що робить їх універсальнішими, проте їх ефективність залежить від складності маніпуляцій.

Жоден із методів не є універсальним, тому найкращі результати дає комбінований підхід, який поєднує кілька методик аналізу. Наприклад, глибокі нейромережі можуть поєднуватися з класичними методами спектрального аналізу або перевірки шумових характеристик камери. Подальші дослідження в цій галузі

спрямовані на створення автоматизованих систем детектування, які зможуть працювати в реальному часі та аналізувати великі обсяги цифрових даних.

## 2.3 Порівняння PixelProfile з іншими програмами для обробки відео- та фотоінформації.

У цьому розділі мною представлено огляд кількох популярних інструментів для виявлення фальсифікацій у цифрових зображеннях, а також аналіз їхніх переваг і недоліків у порівнянні з PixelProfile.

Izitru – це онлайн-сервіс для перевірки справжності зображень, який аналізує шість різних параметрів файлу для виявлення змін. Його основний плюс – швидкість та автоматизована перевірка, проте додаток не дає детального аналізу редагування, а лише підтверджує або спростовує можливу підробку [19]. Відмінність від PixelProfile полягає в тому, що останній дозволяє досліджувати зображення більш глибоко, зокрема на рівні кольорових каналів.

Одним із найпопулярніших інструментів є FotoForensics – це онлайн-платформа, яка надає користувачам можливість виконувати аналіз рівня помилок (ELA) (див. рис. 2.6). Також вона дає можливість перевіряти метадані зображень та знаходити аномалії у стисненні JPEG [20]. Програма є простою у використанні, але водночас обмежується базовими методами перевірки. У порівнянні з реалізованою версією PixelProfile, FotoForensics менш ефективний у детальному спектральному аналізі, але є швидшим для поверхневого виявлення редагування.

Рисунок 2.6 – Приклад аналізу зображення за допомогою рівня помилок [21]

Forensically – це ще один веб-додаток, що дозволяє потенційному клієнту аналізувати рівень помилок, знаходити клоновані області за допомогою методу Copy-Move, перевіряти рівень шуму та витягувати приховані деталі із зображення [22]. Цей інструмент має широкий набір функцій, але оскільки він є веб-додатком, то залежить від стабільного інтернет-з'єднання користувача (див. рис. 2.7).

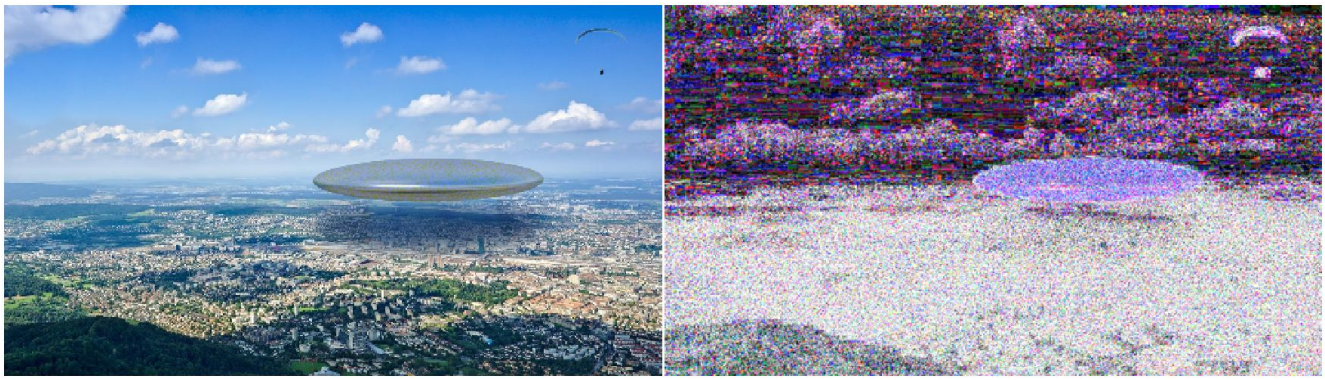


Рисунок 2.7 – Forensically (ELA) виявляє вставлений об'єкт (НЛО) як аномалію

Таким чином, я вважаю що, PixelProfile має свої переваги, зокрема спектрозональний аналіз, який є унікальним підходом для перевірки аерофотознімків та супутникових зображень. Водночас інші програми пропонують інструменти для аналізу рівня помилок, перевірки метаданих та виявлення дубльованих фрагментів, що може бути корисним у загальному аналізі фотографій. Кожен із розглянутих інструментів має свою ідею, і найкращі результати можна отримати, комбінуючи кілька методів аналізу залежно від поставленої задачі.

# 3 РОЗРОБКА ТА ВДОСКОНАЛЕННЯ ПРОГРАМИ PIXELPROFILE ДЛЯ ВИЯВЛЕННЯ МОДИФІКАЦІЙ У ЗОБРАЖЕННЯХ

## 3.1 Визначення обмежень програми на Delphi та переваги переходу на Java.

Розроблений у Delphi 7 у 2003 році, PixelProfile є спеціалізованим інструментом для цифрового аналізу зображень, особливо для спектрального аналізу компонентів RGB з метою виявлення змін на супутникових та аерофотознімках. Його вихідний код, протестований на відповідність військовому стандарту MIL-STD-150A, доступний в Інтернеті, що свідчить про його початкову відкритість і прагматичну цінність. Сучасні потреби в обробці великих і складних зображень, однак, виявили кілька важливих обмежень у цій реалізації, які перешкоджають її ефективному використанню для спектральної розвідки і виявлення хакерських атак [23].

Delphi 7, вперше випущений у 2002 році, є застарілою технологією, яку Embarcadero більше не підтримує, тому він не має офіційної підтримки, патчів безпеки або оновлень. Це ставить під загрозу надійність програми, особливо в контексті кібербезпеки, де захист від вразливостей є життєво важливим. Доступ до сучасних бібліотек обробки зображень, таких як OpenCV, майже неможливий через відсутність активної спільноти, що також ускладнює вирішення технічних проблем та адаптацію до нових вимог. Крім того, основною операційною системою програми є Windows, що обмежує її використання на інших операційних системах, таких як macOS або Linux, і обмежує гнучкість користувачів у різних середовищах, таких як академічні або дослідницькі установи [24]. Програмне забезпечення може бути складнішим у використанні, особливо для професіоналів, які потребують швидкого доступу до аналітичних функцій, через недостатню інтуїтивність та простоту користувацького інтерфейсу, який, ймовірно, був створений з використанням застарілих інструментів Delphi, таких як VCL.

Перехід на Java має низку переваг, які вирішують ці проблеми та відкривають нові можливості для вдосконалення PixelProfile. Oracle та велика спільнота активно підтримують Java - сучасну мову програмування, яка гарантує часті оновлення, патчі безпеки та доступ до нових функцій. Ширша аудиторія може отримати доступ

до PixelProfile, а команди, що використовують різні операційні системи, можуть легше співпрацювати, оскільки Java-додатки можуть працювати на будь-якій платформі - Windows, macOS, Linux тощо. - завдяки віртуальній машині Java (JVM) [25]. Крім того, Java надає користувачам доступ до складних бібліотек, таких як OpenCV, які пропонують розширений спектральний аналіз даних, виявлення аномалій і навіть інтеграцію з алгоритмами машинного навчання, що є важливим компонентом для автоматичного виявлення модифікацій зображень. При роботі з супутниковими знімками високої роздільної здатності висока продуктивність Java, досягнута завдяки JIT-компіляції та підтримці багатопотоковості, дозволяє ефективно обробляти великі набори даних і скорочує час аналізу. Довгострокова життєздатність програми та її адаптивність до нових вимог, таких як інтеграція з хмарними сервісами або веб-перевірка зображень за допомогою GPS-даних, забезпечується великою спільнотою розробників Java, що дозволяє легко знаходити ресурси та розробників для підтримки та оновлень. Крім того, Java надає розширені фреймворки графічного інтерфейсу, такі як JavaFX, які дозволяють розробляти більш зручний та естетично привабливий інтерфейс, покращуючи користувацький досвід та розширюючи доступність аналітичних функцій на різних пристроях, включаючи ноутбуки та планшети [26].

Оскільки він не тільки усуває обмеження застарілої версії Delphi, але й розширює її функціональність, перенесення PixelProfile на Java має практичний сенс. Інтеграція з OpenCV, наприклад, дозволить використовувати складні алгоритми, такі як логарифмічне перетворення для покращення видимості прихованих артефактів або аналіз Фур'є для виявлення швів - обидва ці алгоритми важливі для виявлення хакерських модифікацій. Підвищена продуктивність зробить додаток потужним інструментом для обробки великих зображень, а крос-платформенна сумісність дозволить ширше використовувати його в таких сферах, як кібербезпека, розвідка та наукові дослідження.

3.2 Реалізація методів аналізу зображень.

3.2.1 2D-RGB аналіз зображення.

Реалізація 2D-RGB аналізу є одним з важливих етапів розробки програми PixelProfile, яка дозволяє досліджувати цифрові зображення з точки зору значень пікселів та кольорів. Основною метою такого аналізу є виявлення місць, де зображення були модифіковані, зокрема, хакерського втручання в супутникові або аерофотознімки.

2D-RGB аналіз базується на статистичному дослідженні розподілу кольорів у каналах RGB. Колірні профілі формуються шляхом порівняння інтенсивності червоного (R), зеленого (G) і синього (B) кольорів у вибраних областях зображення. Наприклад, на наступному малюнку показано, як використовувати PixelProfile для дослідження ділянки, яку можна модифікувати (див. рис. 3.1).

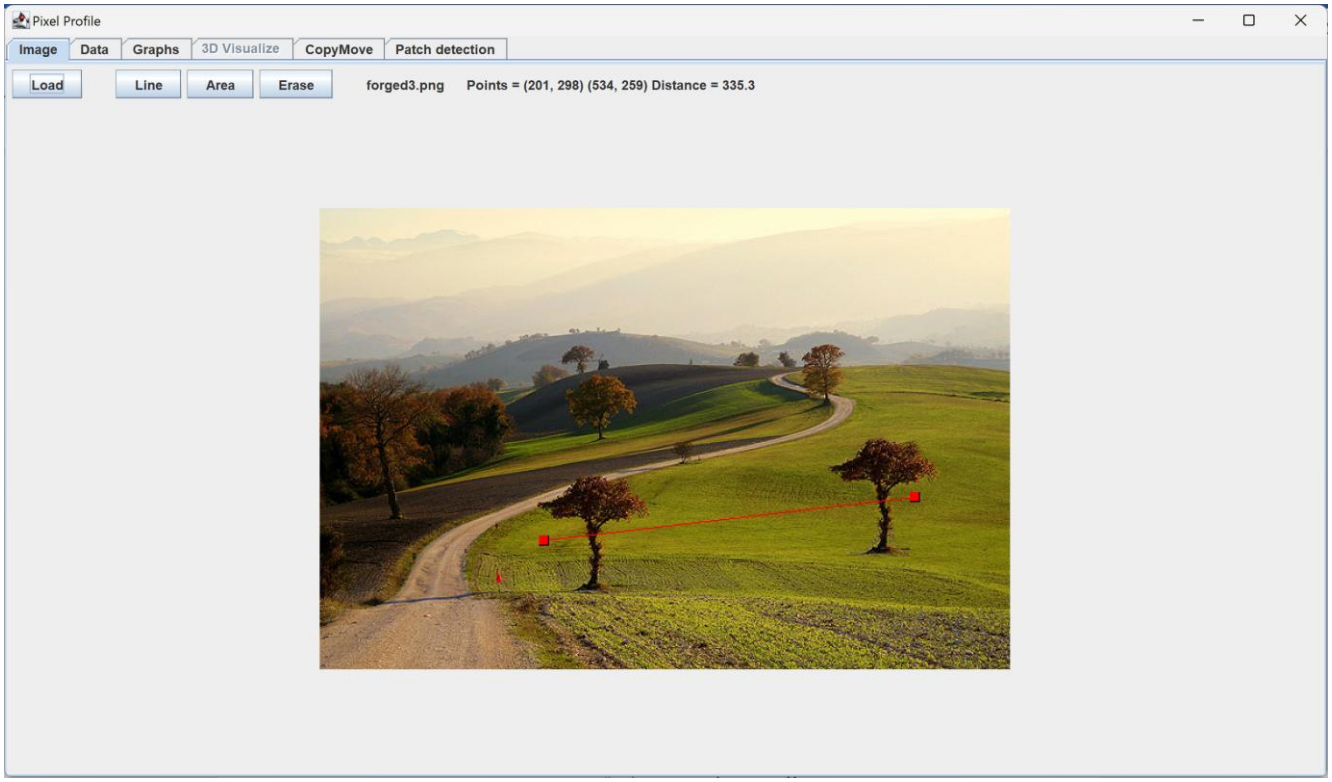



Рисунок 3.1 – Модифіковане зображення

Для аналізу вибирається певна ділянка зображення, а потім виконується детальне порівняння колірних значень цієї ділянки з фоном. В результаті програма видає графіки, що показують зміну інтенсивності кольору вздовж обраної ділянки. На графіку вище видно, що в спектрі зеленого кольору чітко простежуються

аномальні піки, які не можна пояснити природними змінами ландшафту або освітлення, що свідчить про потенційні ознаки втручання

Реалізований алгоритм також дозволяє виявляти сліди так званих «плям», коли фрагменти зображення маскуються під навколишній фон. Однак, завдяки відмінностям у спектральній насиченості та розподілі кольорів, межі таких ділянок досить легко виявити. Цей ефект продемонстровано на скріншоті програми, де на графіку спектральних характеристик очевидна межа між оригінальною частиною зображення і вставленою ділянкою (див. рис. 3.2).

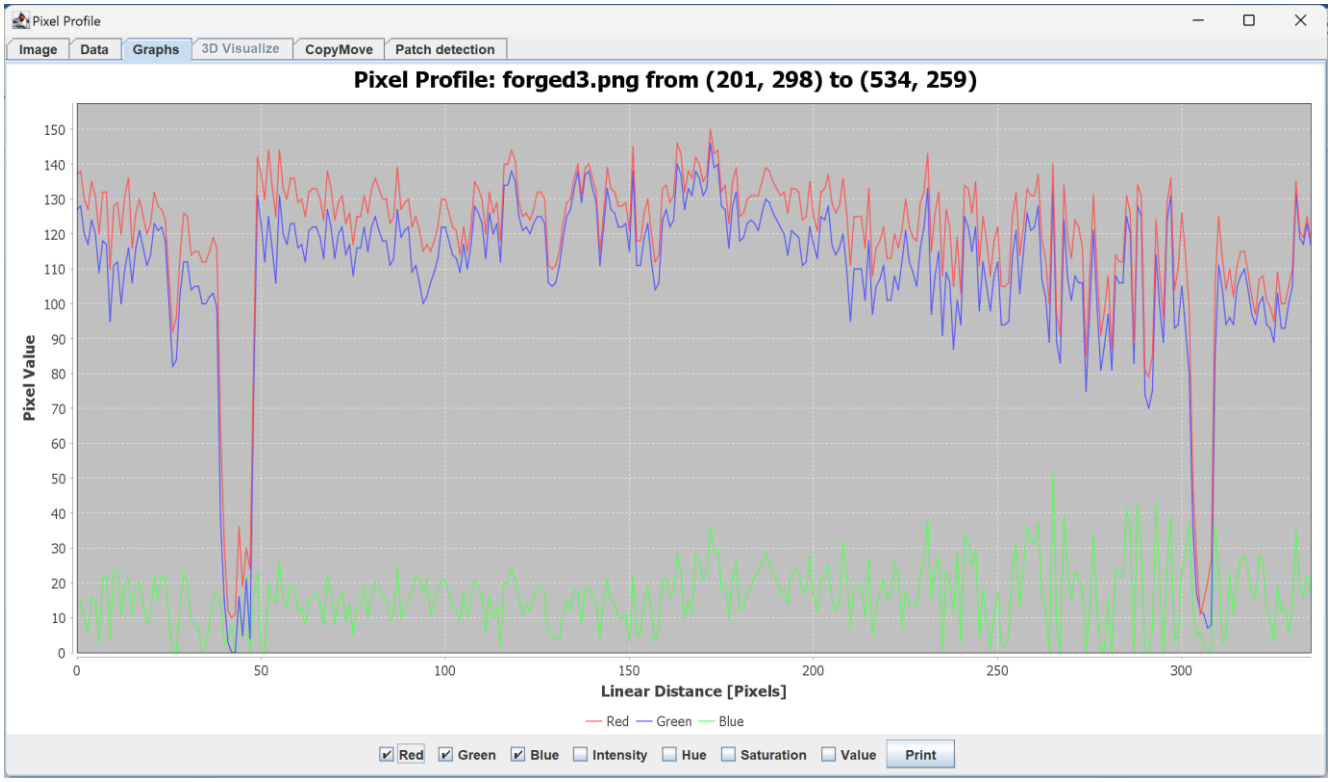



Рисунок 3.2 – Графік модифікованої ділянки

У програмному коді реалізована можливість завантаження зображень, вибору області аналізу через графічний інтерфейс і подальшого створення 2D колірних профілів. Програма будує та відображає графіки на основі XYSeries за допомогою бібліотеки JFreeChart, яка забезпечує якісну візуалізацію та детальну статистику значень кольорів. Взаємодія користувача з графіком дозволяє швидко змінювати та аналізувати різні частини зображення, забезпечуючи точність та ефективність дослідження [27].

Таким чином, впровадження 2D-RGB аналізу в PixelProfile забезпечує більш глибокий рівень перевірки цифрових зображень, значно покращуючи можливості автоматичного виявлення модифікацій і надаючи потужний інструмент для спектрального аналізу в різних сферах діяльності.

### 3.2.2 3D-RGB аналіз зображення.

Реалізація 3D-RGB аналізу стала важливим кроком у розвитку програмного забезпечення PixelProfile, що надає потужні інструменти для тривимірного дослідження спектральних властивостей цифрових зображень. Основною метою такого аналізу є детальне виявлення місць модифікації зображень, особливо в контексті виявлення хакерських втручань у супутникові та аерофотознімки [28].

На відміну від традиційного двовимірного аналізу, 3D-RGB аналіз дозволяє будувати тривимірні моделі, які показують розподіл інтенсивності кожного з трьох колірних каналів (червоного, зеленого і синього) у вибраній області. За допомогою програми PixelProfile оператор може вибрати прямокутну ділянку зображення, після чого виконується аналіз, результатом якого є тривимірне відображення інтенсивності кольору (див. рис. 3.3).

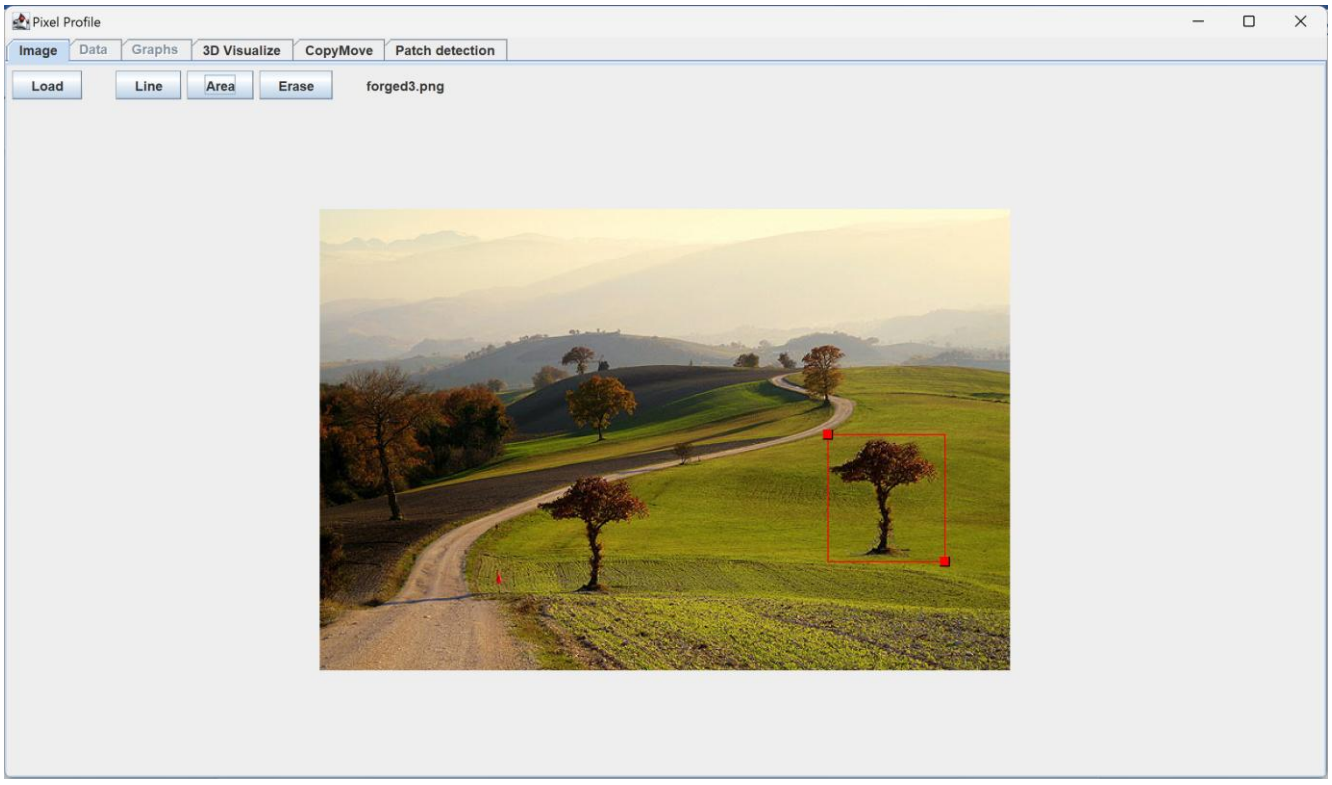



Рисунок 3.3 – Модифіковане зображення

Модифікована версія програми надає можливість масштабування та обертання отриманих тривимірних моделей, що дозволяє дослідникам вивчати деталі спектральної структури зображення під різними кутами огляду (див. рис. 3.4). Така візуалізація значно полегшує виявлення аномалій і допомагає ідентифікувати штучні модифікації, які зазвичай важко помітити при стандартному перегляді.

Наприклад, результати аналізу в каналах RGB наочно демонструють відмінності в спектральних характеристиках окремих ділянок, що свідчить про можливі вставки або замасковані «латки». У разі логарифмічного масштабування рівнів яскравості ці відмінності стають ще більш очевидними для оператора, оскільки людське око сприймає зміни яскравості в логарифмічному масштабі.

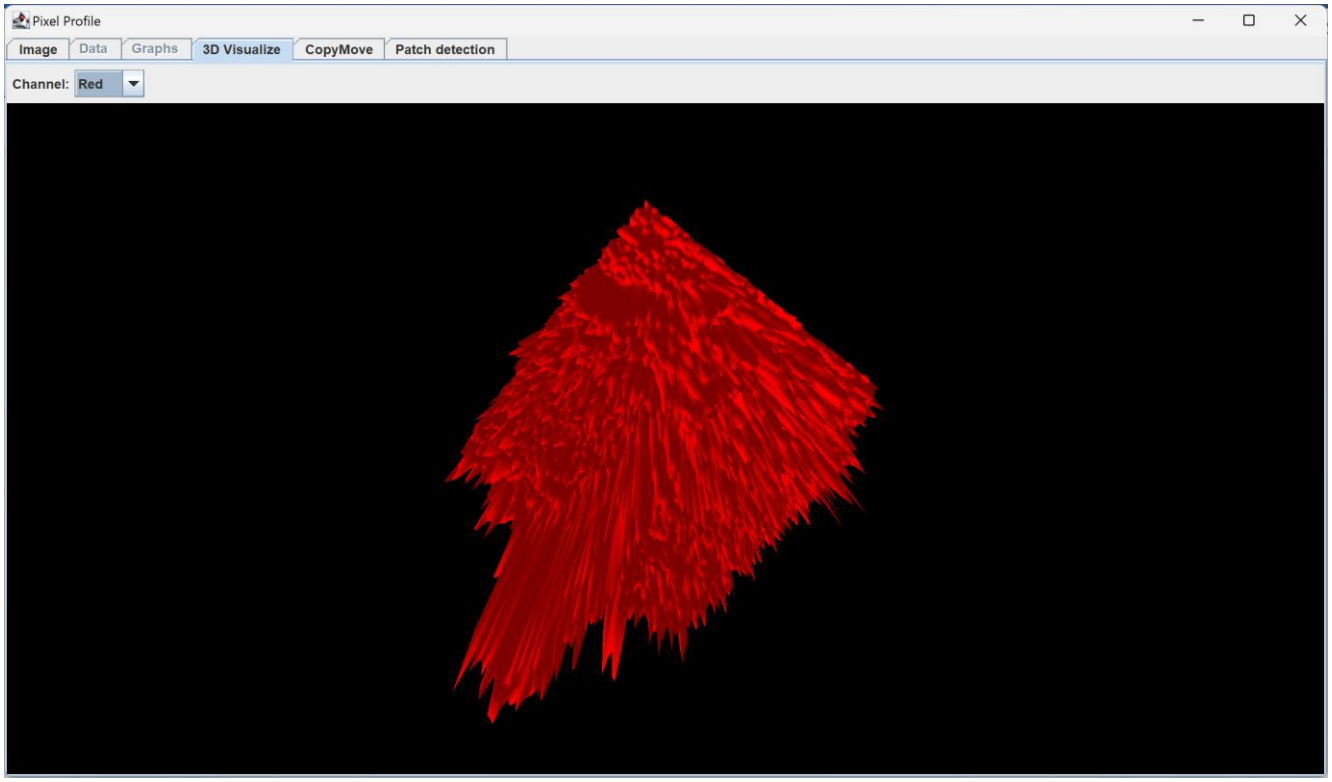



Рисунок 3.4 – Тривимірне відображення кольорової інтенсивності

Результати експериментів з програмою підтвердили високу ефективність 3D-RGB аналізу, особливо в поєднанні з Фур'є-аналізом, що дозволяє виявляти навіть незначні спектральні аномалії. Отримані дані можуть бути використані для автоматизованої перевірки цифрових зображень, виявлення фактів їх модифікації,

а також у перспективних дослідженнях в галузі стеганографії та цифрової криміналістики.

### 3.2.3 Фур'є-аналіз зображення

Метод Фур'є-аналізу є цікавим інструментом, який дозволяє розкласти зображення на синусоїдальні складові, що представляють інформацію в частотній (спектральній) області. Основна ідея цього методу полягає в перетворенні складних просторових сигналів на їхні спектральні складові, що полегшує деякі обчислювальні процеси, такі як згортка або фільтрація [29].

Незважаючи на свої теоретичні переваги та широке застосування в багатьох галузях, включаючи цифрову обробку сигналів, в практичних задачах аналізу зображень, зокрема в програмі PixelProfile, використання Фур'є-аналізу має суттєві обмеження. Основна проблема полягає в тому, що спектральна інформація зображень у Фур'є-області часто є складною для інтерпретації людиною, оскільки більшість реальних зображень містять складні частотні складові, які виглядають хаотично в спектральній області.

Крім того, Фур'є-аналіз є неефективним для виявлення чітких меж модифікованих ділянок зображення, оскільки основні ознаки модифікацій (наприклад, краї об'єктів або вставки фрагментів) представлені в широкому діапазоні частот, що не дозволяє однозначно ідентифікувати їх за допомогою лише частотного спектру. Крім того, як показують результати досліджень та експериментів, навіть при наявності чітко виражених стиків або вставок на зображеннях, спектральна область має розподіл, який важко інтерпретувати без додаткових процедур, таких як логарифмічне перетворення або порогове перетворення спектра.

Враховуючи ці фактори, застосування Фур'є-аналізу в рамках даного проекту є недоцільним, оскільки метод не дає достатньої інформації для ефективного виявлення та ідентифікації місць модифікацій на зображеннях. Це підтверджується науковими джерелами, які вказують на складність та обмеженість інтерпретації спектральних даних у практичних задачах цифрового аналізу зображень.

## 3.3 Розробка алгоритмів для виявлення модифікацій.

### 3.3.1 Розробка алгоритму виявлення Copy-Move Forgery

Метод підробки Copy-Move - один з найпоширеніших видів маніпуляцій з цифровими зображеннями, при якому частина зображення копіюється і вставляється в іншу частину того ж зображення з метою приховати або змінити певні об'єкти або деталі сцени [30].

Для вирішення проблеми виявлення такого типу підробок було запропоновано алгоритм на основі дискретного косинусного перетворення (ДКП), ключових точок, сегментації пікселів та геометричних перетворень Гельмерта. Основна ідея цього методу полягає в аналізі схожості між різними частинами зображення за допомогою алгоритмів пошуку відповідностей між ключовими точками, які попередньо вибираються методом SIFT (Scale-Invariant Feature Transform - масштабно-інваріантне перетворення ознак).

Алгоритм складається з кількох етапів:

1) На початку обробки зображень застосовується метод SIFT, який дозволяє визначити характерні точки та обчислити для них відповідні дескриптори. Далі, використовуючи критерій співвідношення відстаней до найближчих сусідів (Nearest Neighbor Distance Ratio), обираються ті пари точок, чиї дескриптори мають найвищу схожість, і формуються відповідні відповідності між зображеннями.
2) Після попереднього етапу формуються кілька груп парних точок, які відповідають схожим фрагментам зображення. Однак у ході експериментів з’ясувалося, що початкова кластеризація не завжди точно об’єднує точки, які насправді належать до однієї області. Щоб усунути цю неточність, було додано етап об’єднання груп на основі геометричних перетворень Гельмерта. Це дозволило суттєво підвищити точність виявлення змінених або фальсифікованих ділянок.
3) Щоб забезпечити більш точне визначення меж змінених фрагментів, застосовується суперпіксельна сегментація методом SLIC (Simple Linear Iterative Clustering). Завдяки цьому вдається мінімізувати похибки при виявленні областей копіювання та вставки. Після сегментації межі додатково

уточнюються з використанням перетворення Гельмерта, що дозволяє досягти високої точності локалізації маніпульованої ділянки.

На рисунку нижче показано результат роботи алгоритму на прикладі ландшафтного зображення, де одне з дерев було скопійовано та вставлено в інше місце (див. рис. 3.5). Після застосування алгоритму чітко виділяються дві ідентичні ділянки, що підтверджує ефективність запропонованого методу.

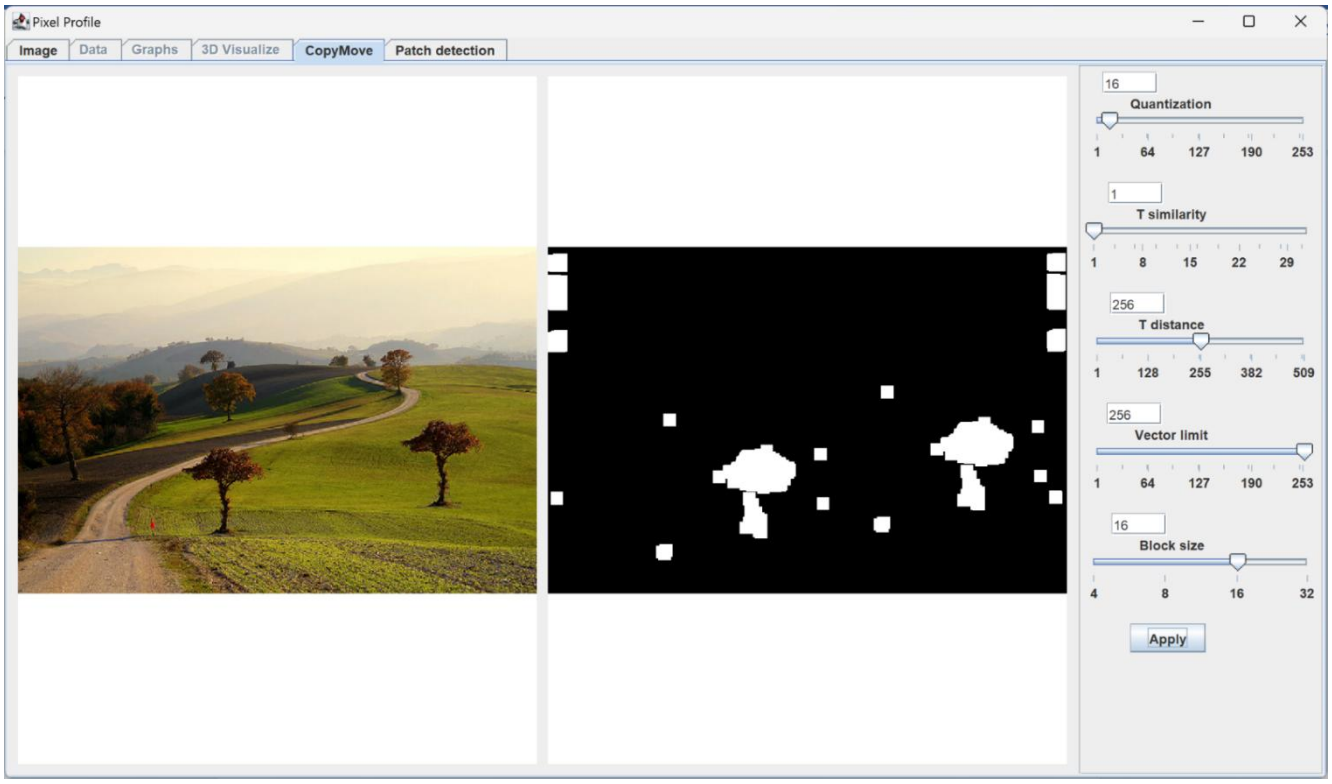



Рисунок 3.5 – Результат роботи алгоритму на прикладі зображення ландшафту

Важливо відзначити, що запропонований метод демонструє високу ефективність як для простих копій, так і для обертання вставленого фрагмента. Однак його поточна версія має обмеження у вигляді наявності масштабування вставлених фрагментів. Це обмеження буде усунуто в наступних версіях розробленого програмного забезпечення шляхом застосування додаткових методів незалежного від масштабу аналізу.

Були проведені додаткові експерименти з використанням різноманітних тестових наборів зображень, включаючи автомобілі та інші технічні об'єкти, щоб оцінити ефективність запропонованого алгоритму в різних умовах. На рисунку 2.6 показано результати тестування зображення автомобіля, де автомобіль було

скопійовано та вставлено з іншого боку. Алгоритм успішно виявив та локалізував області копіювання (див. рис. 3.6).

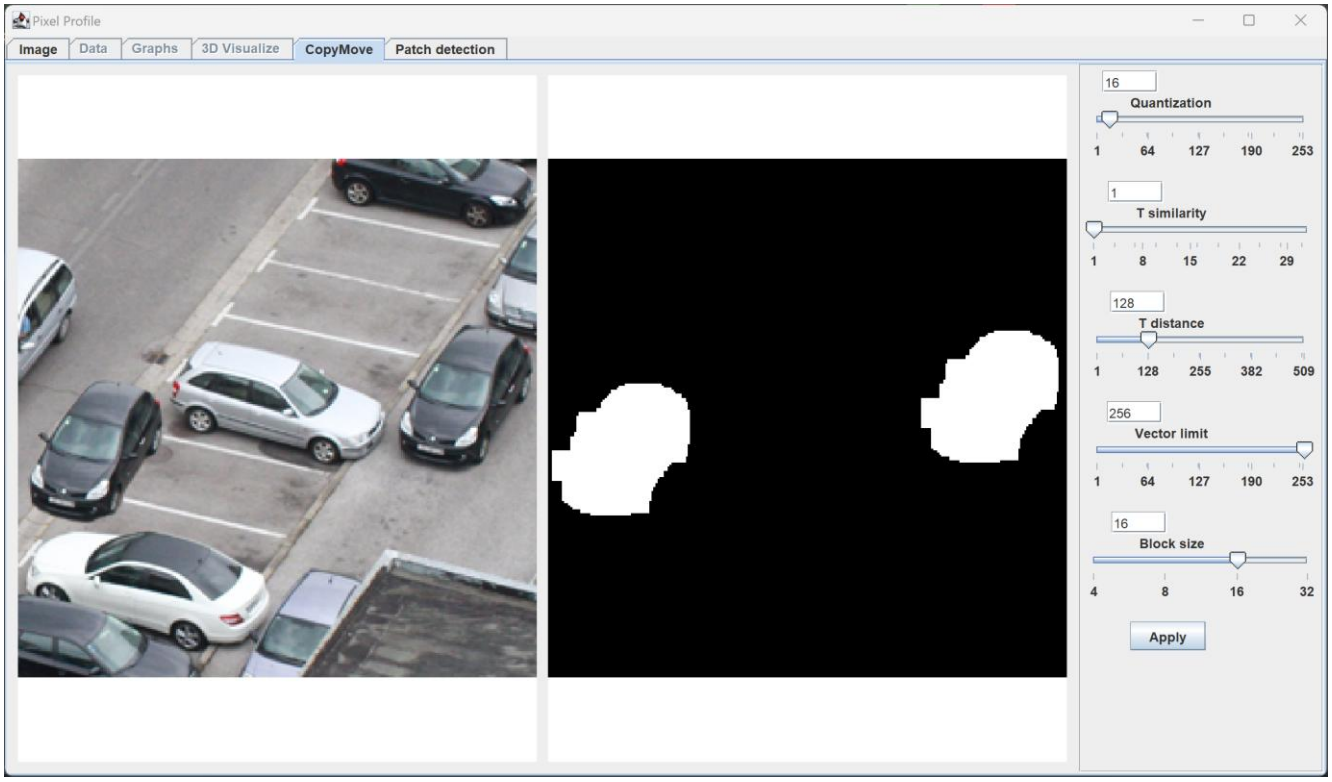



Рисунок 3.6 – Результат роботи алгоритму на прикладі

Таким чином, запропонований у цьому дослідженні алгоритм забезпечує ефективне виявлення підробок методом «копіювання-переміщення», включаючи випадки з геометричними перетвореннями, окрім масштабування. Він є перспективним інструментом для подальшого дослідження та вдосконалення і має великий потенціал для практичного застосування в криміналістичних та інших спеціалізованих системах виявлення цифрових підробок.

### 3.3.2 Пошук вставлених фрагментів на зображенні.

Однією з найпоширеніших і найпідступніших форм цифрового втручання є склеювання - процес вставки частин інших зображень або штучно згенерованих елементів в оригінальне зображення. На відміну від іншого типу маніпуляцій, Copy-Move, коли фрагмент копіюється і вставляється в межах одного зображення, сплайсинг передбачає інтеграцію «чужорідного» контенту, який походить з іншого джерела і не має дублікату в оригінальному тлі.

Виявлення склеювання є складним завданням, оскільки візуально добре виконана вставка може бути невидимою для неозброєного ока. Тому пасивні (сліпі) методи цифрової криміналістики зосереджені на пошуку прихованих артефактів і статистичних невідповідностей, які неминуче виникають у процесі редагування. Ці методи поділяються на дві основні категорії: ті, що аналізують межі вставки (boundary-based), і ті, що досліджують вміст регіону (region-based).

Підходи до виявлення сплайсингу:

1) Аналіз меж вставки (Boundary-Based Methods). Ці методи базуються на припущенні, що на кордоні між оригінальним фоном та вставленим фрагментом можуть виникати аномалії, навіть якщо візуально межа згладжена. Такими аномаліями можуть бути:
   - Невідповідність різкості: Межа може бути занадто різкою або, навпаки, штучно розмитою (наприклад, за допомогою фільтра блюр) для приховування слідів вирізання. Аналіз розподілу різкості вздовж контурів зображення може виявити такі неприродні переходи.
   - Артефакти на контурах: Використання операторів виділення контурів (як-от Sobel або Canny) дозволяє знайти потенційні межі. Подальший аналіз цих контурів – оцінка їхньої різкості, спектру частот, або різниці характеристик по обидва боки – може вказати на штучне походження межі [31].
   - Аналіз розмиття (Blur Analysis): Дослідження розподілу та типу розмиття (наприклад, розмиття фокусу, розмиття в русі) вздовж країв може виявити області, де розмиття було застосовано навмисно для маскування вставки.
   - Візуальна помітність: Вставлені об'єкти можуть створювати контури або текстури, які не повністю узгоджуються з оточенням і привертають увагу алгоритмів виявлення візуальної помітності, що також може слугувати ознакою фальсифікації.
2) Аналіз вмісту області (Region-Based Methods). Ці методи фокусуються на пошуку внутрішніх статистичних невідповідностей в межах самого потенційно вставленого фрагмента порівняно з рештою зображення.

Оскільки фрагмент походить з іншого джерела (іншої камери, іншого освітлення, іншого процесу обробки), він може мати інший "цифровий почерк". До таких методів належать:

- Аналіз шуму та різкості: Кожна камера має свій унікальний шумовий профіль та особливості передачі різкості. Вставлений фрагмент з іншого джерела може мати інший рівень або характер шуму (наприклад, фотонний шум, шум зчитування), а також відрізнятися за рівнем різкості через різний фокус чи об'єктив. Аналіз локальної дисперсії шуму або градієнтів різкості може виявити такі розбіжності.
- Перевірка колірних характеристик та освітлення: Невідповідності в балансі білого, відтінках кольорів, напрямку та інтенсивності освітлення між вставкою та фоном можуть бути сильними індикаторами фальсифікації. Аналіз тіней, відблисків або порівняння гістограм кольорів можуть допомогти виявити такі аномалії.
- Аналіз статистик камери: Деякі методи використовують знання про специфічні процеси формування зображення цифровими камерами. Наприклад, артефакти демозаїки (пов'язані з Color Filter Array - CFA) або унікальний шаблон шуму сенсора (Photo-Response Non-Uniformity - PRNU) є характерними для конкретної камери. Невідповідність шаблонів CFA або значне падіння кореляції PRNU в певній області зображення можуть вказувати на вставку з іншого пристрою [32].
- Аналіз JPEG-артефактів: Зображення, збережені у форматі JPEG, містять специфічні артефакти, пов'язані з процесом стиснення. Якщо вставлений фрагмент мав інший рівень стиснення або все зображення було повторно стиснуто після вставки, це може призвести до ефекту подвійного стиснення, який проявляється у змінах в розподілі коефіцієнтів дискретного косинусного перетворення (DCT) або гістограмах квантованих значень. Аналіз параметрів JPEG в різних частинах зображення дозволяє локалізувати місце монтажу.

У контексті розробки інструментів для виявлення зрощування, зокрема на супутникових знімках, у програмі PixelProfile було реалізовано алгоритм, що базується на оцінці локальної дисперсії різкості. Принцип методу базується на тому, що багато «латок», особливо на супутникових знімках, створюються шляхом розмивання, зафарбовування або згладжування певних ділянок (наприклад, для приховування військових об'єктів). Такі штучно оброблені ділянки зазвичай мають меншу дисперсію градієнта, тобто виглядають більш гладкими порівняно з природним, текстурованим середовищем.

Алгоритм працює наступним чином:

1) Зображення перетворюється у градації сірого.
2) Обчислюються градієнти різкості за допомогою оператора Лапласа, який чутливий до змін інтенсивності пікселів.
3) Зображення ділиться на невеликі блоки фіксованого розміру (наприклад, 64x64 пікселі).
4) Для кожного блоку обчислюється дисперсія значень градієнтів різкості. Низька дисперсія вказує на відносну однорідність (гладкість) вмісту блоку.
5) Блоки, дисперсія яких виявляється нижчою за заданий пороговий рівень, позначаються як підозрілі (наприклад, їм присвоюється максимальне значення в масці результату). Порогове значення дисперсії підбирається таким чином, щоб відсікти фонові коливання, не пов'язані з фальсифікацією.
6) Застосовується операція морфологічного закриття для об'єднання сусідніх підозрілих ("гладких") блоків у більші, цілісні області, що можуть відповідати "латкам".

Результатом є маска або візуалізація, яка виділяє ділянки з низькою дисперсією різкості, що є потенційними місцями для вставки або редагування. У практичному прикладі, описаному в тексті (див. рис. 3.7), метод успішно ідентифікував штучно згладжену центральну область супутникового знімка.

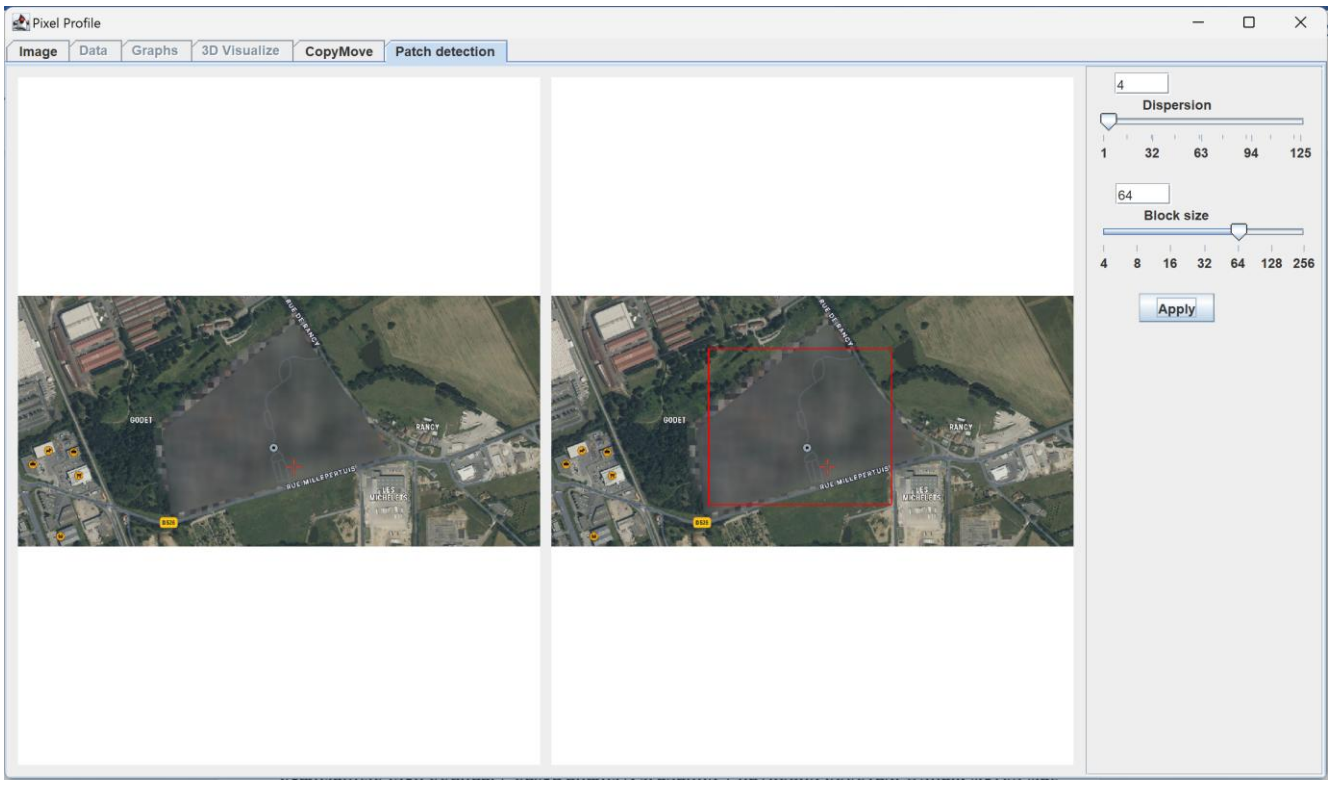



Рисунок 3.7 – Результат роботи алгоритму на прикладі

Розроблений алгоритм у PixelProfile ефективно виявляє спроби маскування шляхом згладжування, розмивання, розфарбовування або цензурування. Це спрощена реалізація ідей граничного аналізу, які згадуються в наукових роботах. Однак метод має обмеження: він не може виявити вставлені фрагменти, які мають таку ж складність текстури, рівень шуму та розподіл різкості, як і навколишній фон. Наприклад, якщо вставка містить природні текстури (ліс, будівлі) або була вставлена з джерела зі схожими характеристиками різкості, градієнтна дисперсія може не відрізнятися від фону, і метод не спрацює.

Більш складні наукові підходи часто поєднують кілька функцій для підвищення надійності виявлення. Ці функції можуть включати аналіз розмиття країв, невідповідності спектру шуму, аналіз неприродних меж сегментів і використання методів машинного навчання (наприклад, FusionBoost, SVM) для інтеграції результатів з різних дескрипторів. Реалізація PixelProfile, яка використовує лише один дескриптор (локальну дисперсію градієнта), забезпечує низькі обчислювальні витрати та роботу в реальному часі, але не покриває весь спектр можливих сценаріїв шахрайства зі сплайсингу.

Незважаючи на свої обмеження, розроблений алгоритм, заснований на аналізі дисперсії різкості, є цінним інструментом для швидкого виявлення певних типів фальсифікації зображень, включаючи маскування об'єктів шляхом згладжування. Він демонструє ефективність у виявленні специфічних «згладжених» ділянок і легко масштабується для обробки великих зображень.

Плани на подальший розвиток програми PixelProfile включають інтеграцію додаткових, більш складних методів аналізу для підвищення точності та універсальності виявлення сплайсингу. Серед запланованих удосконалень:

- Аналіз кольорового шуму (PRNU) для ідентифікації вставок з іншого джерела.
- Перевірка відповідності JPEG-артефактів у різних ділянках зображення для виявлення ефекту подвійного стиснення.
- Використання інших фільтрів для виділення контурів, таких як Sobel або Canny, для покращення детекції різких або аномальних країв.
- Додавання класифікатора (наприклад, нейронної мережі або SVM), який зможе комбінувати результати аналізу різних ознак для прийняття більш обґрунтованого рішення про наявність фальсифікації та зменшення кількості хибнопозитивних спрацьовувань.

Впровадження цих удосконалень дозволить створити більш надійний та універсальний інструмент виявлення зрощування, здатний аналізувати ширший спектр цифрових слідів, залишених процесом редагування, тим самим підвищуючи довіру до цифрових зображень. Навіть якщо межа вставки візуально невидима, цифрові сліди, які порушують вищу статистику зображення, часто залишаються і можуть бути виявлені за допомогою відповідних алгоритмів.

# 4 ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ НОВОЇ ВЕРСІЇ ПРОГРАМИ

## 4.1 Проведення експериментів із супутниковими знімками.

Для оцінки ефективності вдосконаленої програми PixelProfile було проведено серію експериментів з реальними супутниковими знімками, які моделювали типові випадки редагування - приховування об'єктів шляхом «замазування» або накладання фрагментів з навколишнього фону.

Для експерименту об'єктом дослідження було обрано фрагмент аеродромного покриття військової авіабази, розташованої на території Російської Федерації - зокрема, північну частину аеродрому Енгельс, який відомий як база стратегічної авіації. На супутниковому знімку (див. рис. 4.1), датованому червнем 2023 року, видно два важкі бомбардувальники Ту-95МС, припарковані на відкритих стоянках.


Рисунок 4.1 – Оригінальне зображення аеродрому з літаками [33]

Обрана ділянка має високу структурну регулярність (бетонна плита з ідентичними лініями розмітки), що створює ідеальні умови для спектрального

аналізу - будь-які вставки, спотворення або ретуш на такому фоні легко виявляються через порушення спектральної однорідності. Таким чином, знімок з авіабази в Енгельсі був використаний як тестовий кейс для перевірки здатності програми PixelProfile фіксувати факт модифікації супутникових даних шляхом маскування військової техніки [34].

На наступному етапі зображення модифікували (див. рис. 4.2), скопіювавши фрагмент фону поруч зі злітно-посадковою смугою і розмістивши його над одним із літаків. Такий спосіб редагування є типовим для спроб приховати об'єкти на супутникових знімках.


Рисунок 4.2 – Модифіковане зображення з накладеною «латкою» поверх об'єкта

Візуально межа між оригінальним зображенням і вставленою областю практично непомітна - колірна заливка, характеристики тіней і текстура фону підібрані таким чином, щоб «латка» на місці відсутньої площини виглядала максимально природно. Така маніпуляція є типовою для технік візуального маскування об'єктів, де редагування виконується шляхом копіювання сусідніх фрагментів і накладання їх на цільову область.

Однак при застосуванні методу 2D-RGB аналізу на відрізку прямої лінії, що перетинає змінений сегмент, виявляються яскраво виражені спектральні аномалії - зокрема, спостерігаються різкі пікові відхилення значень інтенсивності кольорових каналів [34]. Найбільш значні коливання фіксуються в зеленому і блакитному каналах, що свідчить про невідповідність спектральної структури між фоновим зображенням і накладеним сегментом (див. рис. 4.3). Такі випромінювання, що утворюються на межі переходу, є характерною ознакою зміненого спектрального профілю пікселів і можуть бути використані як цифровий індикатор стороннього втручання у візуальний зміст зображення.

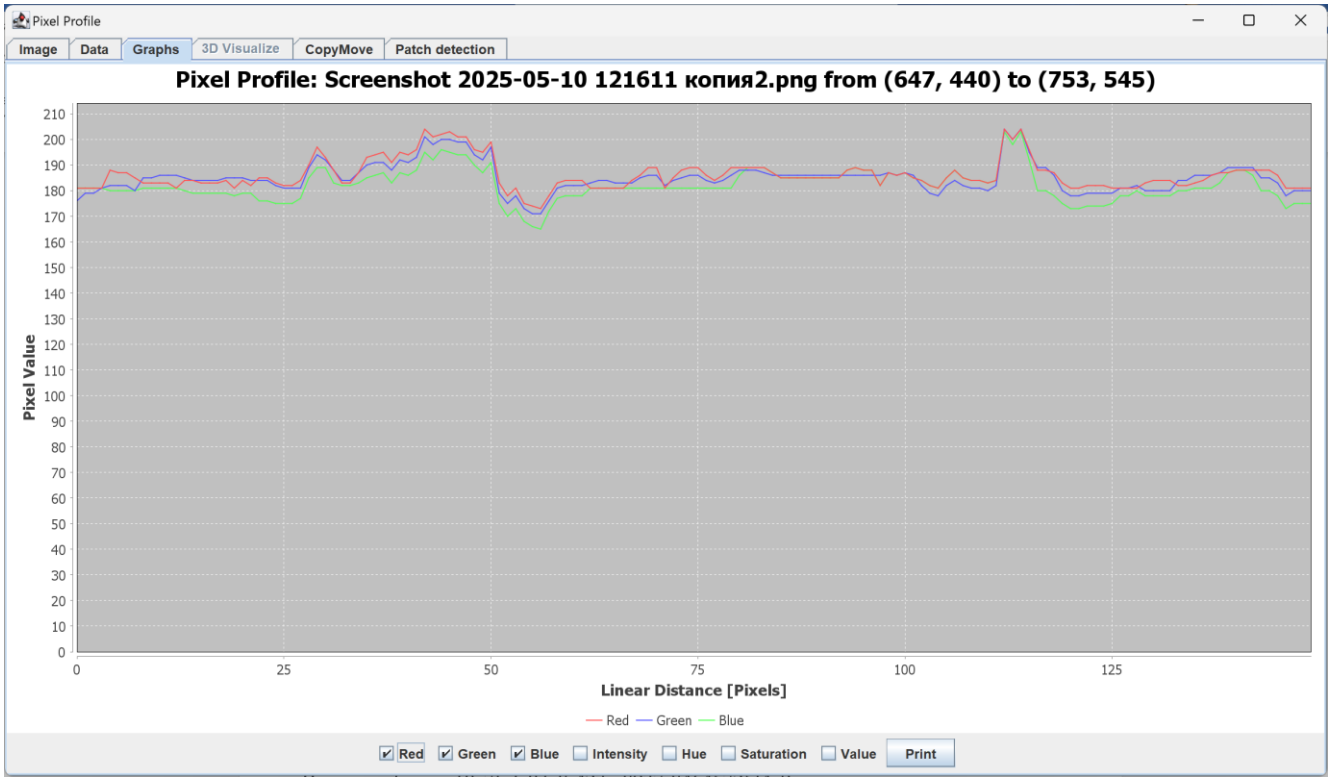



Рисунок 4.3 – Результат 2D-RGB аналізу ділянки: виявлення спектральних аномалій

Для більш детального аналізу та просторової локалізації аномалії була виконана 3D-RGB візуалізація в зеленому каналі. Просторова модель виявила зону підвищеної спектральної енергії, яка чітко контрастує з навколишнім середовищем і корелює з раніше ідентифікованими викидами. Як видно на тривимірному зображенні (див. рис. 4.4), поверхня латки створює спектральну нерівномірність, яка не спостерігається на інших ділянках аеродромного покриття. Це свідчить про

те, що застосований метод дуже чутливий до несанкціонованих змін, навіть у тих випадках, коли редагування виконується з дотриманням візуальної сумісності.

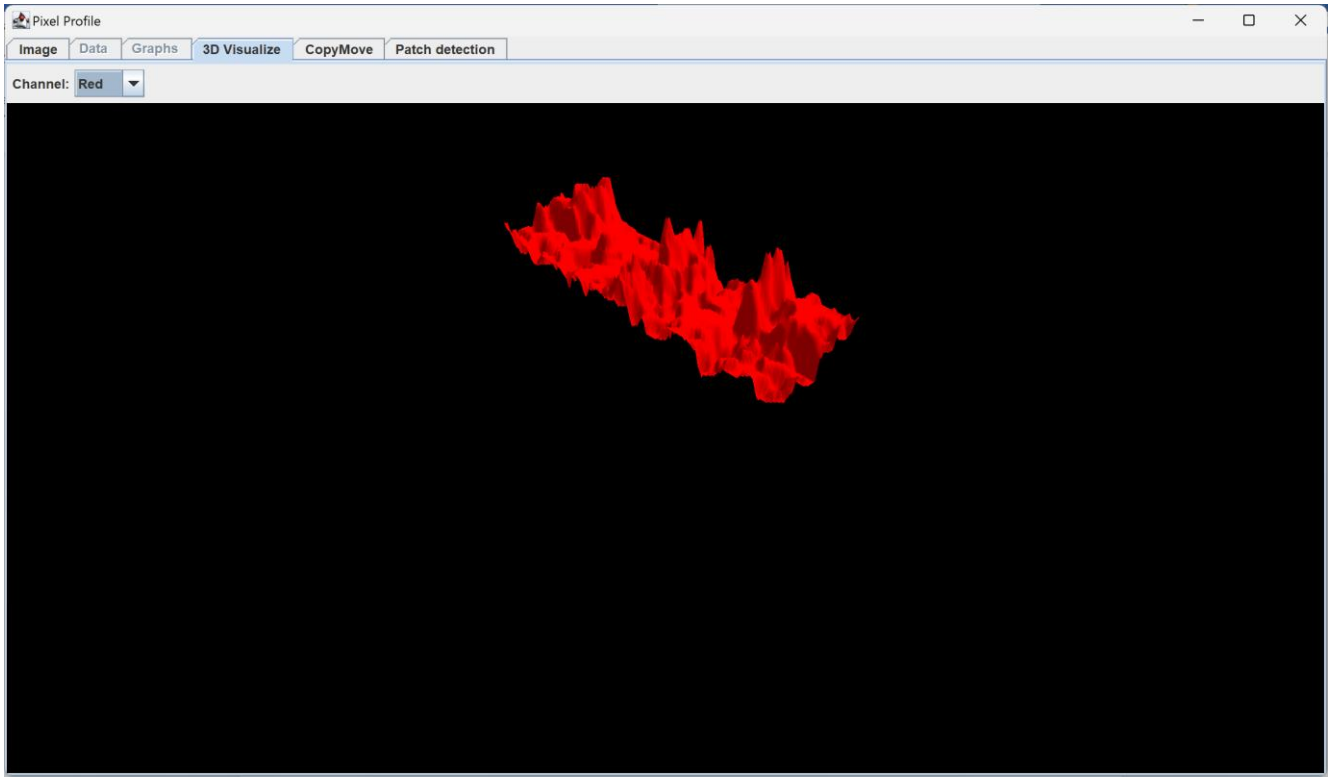



Рисунок 4.4 – 3D-візуалізація ділянки у червоному каналі

Для тестування функціональності алгоритму виявлення копіювання та вставки була змодельована типова ситуація фальсифікації, яка може бути використана противником для створення ілюзії масового зосередження техніки. Зокрема, один з літаків на аеродромі був штучно скопійований і вставлений в нову позицію на тому ж знімку з мінімальною трансформацією (без повороту і масштабування), що імітує тактику інформаційного обману шляхом дублювання об'єктів на супутникових знімках.

Для аналізу я використовував режим CopyMove в PixelProfile, який дозволяє автоматично виявляти ділянки, що мають значний ступінь схожості на рівні блокової структури. Алгоритм працює, розбиваючи зображення на фрагменти заданого розміру (в даному випадку 16×16 пікселів) і шукає відповідні патерни на основі просторової відстані між ними, векторного зсуву та порогової схожості [34].

В результаті аналізу було виявлено три області на зображенні (див. рис. 4.5), які мають ідентичні текстурні характеристики. На правій панелі показано маску

виявлених дублікатів - білі області відповідають ділянкам, які мають значну внутрішню кореляцію і, найімовірніше, є результатом копіювання.

Отримані результати демонструють здатність PixelProfile точно виявляти повторно вставлені об'єкти, навіть якщо фон дуже схожий і структурно регулярний. Це робить метод придатним для виявлення навмисних дублювання або спроб дезінформації у військовій, супутниковій та криміналістичній практиці.

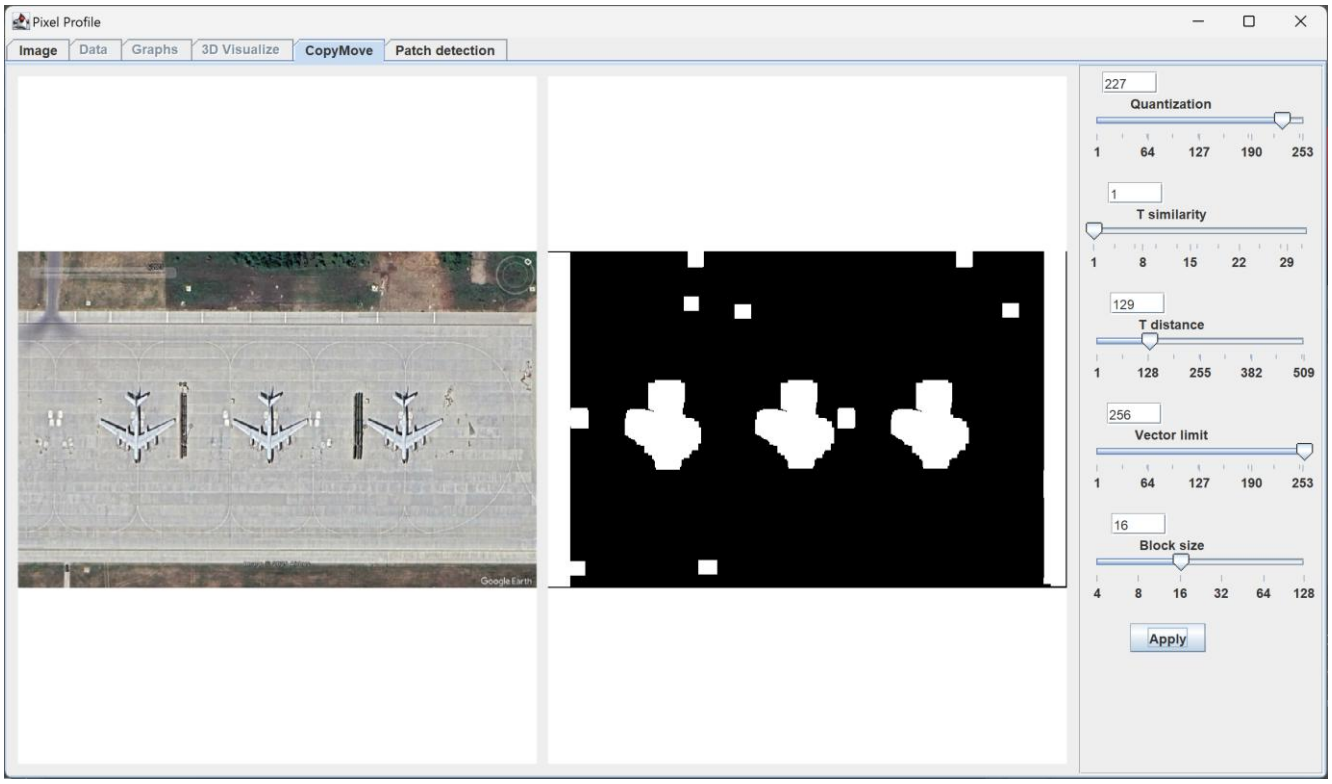



Рисунок 4.5 – Виявлення фрагментів типу CopyMove (дублювання літаків)

Ще один експеримент був присвячений перевірці здатності алгоритму Patch Detection виявляти ділянки, де була зроблена спроба приховати об'єкти шляхом накладання однорідних фонових латок. Цей метод є типовим прийомом цифрової цензури: замість явного видалення об'єкта зображення його накривають фрагментом фону з попередньою фільтрацією, наприклад, розмиванням або копіюванням плитки з іншої області [34].

На тестовому супутниковому знімку аеродрому об'єкти (літаки) були навмисно приховані вручну шляхом накладення спрощених за текстурою ділянок - «латок», які візуально імітують бетонне покриття з незначними змінами кольору та яскравості. Така обробка не викликає підозр при поверхневому перегляді, але

суттєво змінює локальну структуру градієнтів яскравості, що може бути виявлено засобами цифрової криміналістики.

Використаний алгоритм Patch Detection працює шляхом аналізу локальної дисперсії яскравості в межах фіксованих блоків (у цьому випадку 4×4 пікселі). Алгоритм виявляє аномально гладкі ділянки (див. рис. 4.6), де немає нормальних варіацій текстури, характерних для навколишнього середовища. У правій частині інтерфейсу відображаються результати виявлення: червоними рамками позначені ділянки з підозріло низькою дисперсією, що може бути наслідком редагування.

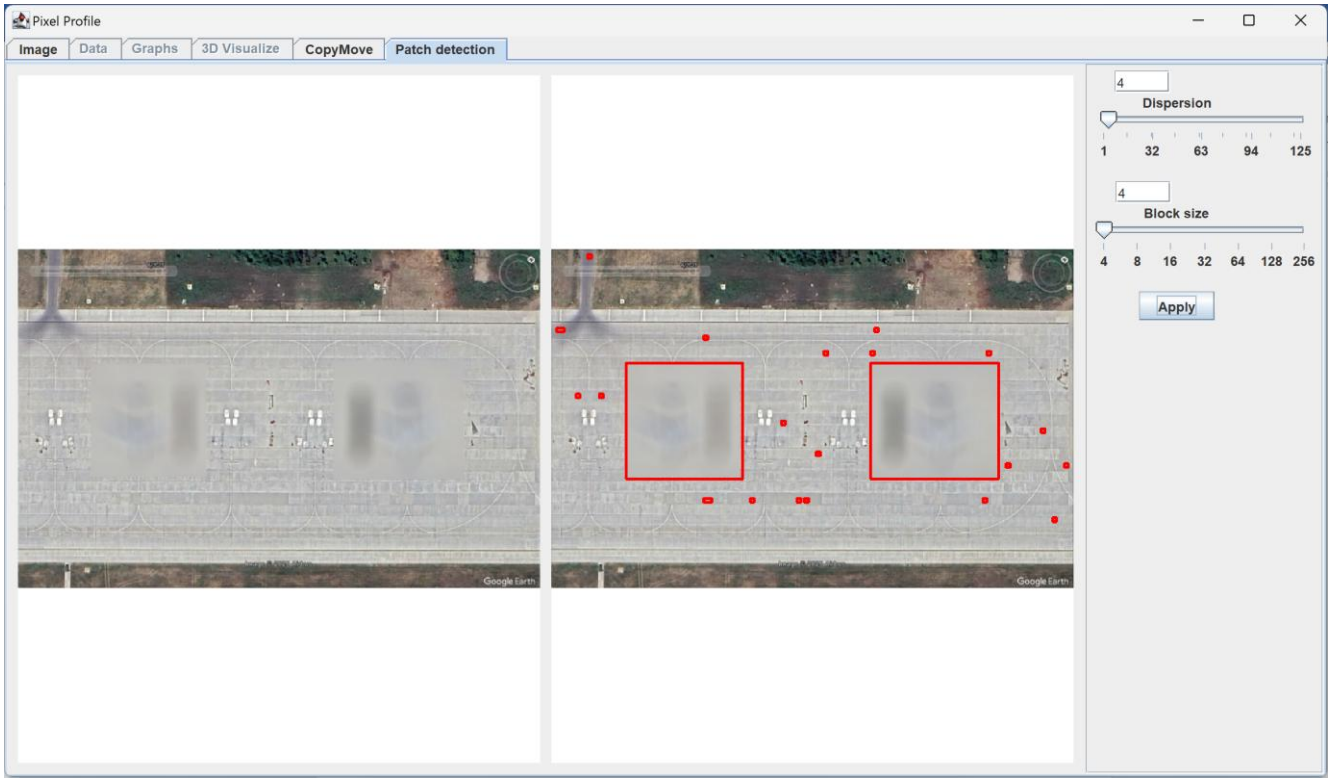



Рисунок 4.6 – Виявлення латок із зниженою дисперсією яскравості

Результати експерименту підтверджують, що навіть при якісному візуальному згладжуванні поверхні алгоритм здатен виявляти «неприродно чисті» ділянки, які порушують спектральну або текстурну узгодженість зображення. Це відкриває можливість автоматизованого виявлення ділянок приховування або підміни інформації на супутникових даних та інших типах фотоматеріалів.

4.2 Порівняння з результатами, отриманими іншими програмами.

Для комплексної оцінки ефективності вдосконаленої версії програми PixelProfile було проведено порівняльний аналіз її результатів з даними, отриманими за допомогою декількох поширених систем цифрової експертизи зображень. Зокрема, для порівняння було обрано веб-інструменти Izitru, FotoForensics, Forensically, а також спеціалізоване програмне забезпечення JPEGSnoop та Ghiro, яке використовується для технічного аналізу зображень, метаданих та особливостей стиснення [35][36].

Знімки, що використовувалися в тестуванні, містили як штучно вставлені об'єкти (копії літаків), так і замасковані ділянки з ділянками фону [37]. Таким чином, експерименти моделювали як сценарії приховування техніки, так і спроби дублювання об'єктів - типові практики дезінформації, що мають місце на геопросторових та супутникових знімках.

Інструмент Izitru показав свою обмеженість у таких випадках. Він орієнтований насамперед на перевірку автентичності JPEG-файлів шляхом аналізу структури зберігання, зокрема наявності первинного хешу та ознак подвійного стиснення. Однак у випадках, коли зображення перекодується у формат PNG або створюється заново після редагування, функціональність Izitru фактично нівелюється - сервіс не надає жодної оцінки реальних візуальних змін. Тому ця програма підходить лише для поверхневої перевірки автентичності JPEG-фотографій, без будь-якої локалізації змін на зображенні.

Інший веб-сервіс, FotoForensics, використовує аналіз рівня помилок (Error Level Analysis, ELA) для виявлення областей неоднорідності в розподілі втрат після стиснення. У деяких випадках ELA дійсно демонструє наявність змін, але не дозволяє точно локалізувати їх або визначити причину - будь-яка перезаписана область буде позначена як «аномальна», навіть якщо редагування було незначним. При тестуванні модифікованого зображення з прихованими літаками FotoForensics вказувала лише загальні ділянки з можливими змінами, не надаючи їх однозначної ідентифікації [38][39].

Значно кращі результати продемонстрував Forensically, який має розширений набір інструментів, включаючи детектори клонів, векторні копії, аналіз шуму та

артефактів JPEG [40]. У випадку багаторазового дублювання літаків метод Clone Detection виявив збіги аж до піксельного рівня. Водночас алгоритм Patch Match, який мав би виявляти штучно згладжені ділянки, не показував результатів у випадках ретельного фону, зокрема, коли структура кольору була близькою до середнього по зображенню. Аналіз шуму та блокових артефактів також показав низьку ефективність у тестах з PNG-зображеннями, що підтверджує обмеженість алгоритмів, прив'язаних до структури JPEG.

На тлі цих інструментів PixelProfile виявився явним переможцем. Працюючи в локальному режимі як десктопна програма, вона забезпечує повноцінний спектральний аналіз з гнучкими налаштуваннями таких параметрів, як розмір блоку, поріг дисперсії та відстань для пошуку копій. Завдяки підтримці як RGB, так і 3D візуалізації спектральної інтенсивності, програмі вдається не тільки виявити факт редагування, але й точно локалізувати змінені ділянки. Всі виявлення супроводжуються аналітичною візуалізацією - графіками інтенсивності пікселів, тривимірними моделями та масками аномалій - що підвищує надійність висновківі.

Під час тестів PixelProfile показав найвищу адаптивність до форматів, гнучкість у налаштуваннях та можливість використання в повністю автономному середовищі, що є критично важливим в умовах обмеженого або закритого доступу до мережі. Це забезпечує високий рівень автономності та конфіденційності - параметри, які особливо актуальні у військовій сфері, супутниковій розвідці та державній експертизі.

Підсумовуючи результати порівняння, можна зробити висновок, що більшість існуючих інструментів фокусуються або на поверхневих ознаках змін (таких як метадані чи стиснення), або на дуже вузькому типі артефактів (ELA, шум JPEG). Натомість PixelProfile демонструє аналітичну глибину, гнучкість і стабільність навіть при роботі з високоякісними, нестисненими форматами. Це робить його конкурентоспроможним інструментом для точного спектрально-орієнтованого аналізу цифрових зображень з можливістю глибокої локалізації зон редагування, чого не може зробити більшість веб-інструментів.

4.3 Висновки щодо точності та ефективності.

На основі експериментів, проведених з використанням реальних та штучно модифікованих супутникових знімків, можна зробити узагальнені висновки про точність та ефективність удосконаленої версії програми PixelProfile для виявлення цифрових маніпуляцій.

Застосовані методи 2D-RGB та 3D-RGB аналізу, реалізовані в програмі, забезпечують високу точність локалізації змінених ділянок на зображенні, що підтверджується як якісною, так і візуальною оцінкою результатів. Програма продемонструвала здатність надійно виявляти спроби приховування об'єктів (патчі), дублювання елементів сцени (Copy-Move) та зменшення локальної варіабельності текстури. Спектральний аналіз колірних каналів дозволив чітко зафіксувати аномалії, які неможливо виявити за допомогою класичних JPEG-орієнтованих інструментів.

Порівняно з іншими поширеними програмами цифрової криміналістики, такими як Izitru, FotoForensics та Forensically, PixelProfile забезпечив вищу деталізацію та точність при роботі з нестисненими (PNG) форматами, що є важливою перевагою для високоякісних супутникових та аерофотознімків. Також було виявлено, що більшість веб-сервісів або не підтримують глибокий спектральний аналіз, або неефективні при виявленні ретельно замаскованих змін.

Додатковою перевагою є те, що PixelProfile є стаціонарним програмним забезпеченням, яке не потребує підключення до Інтернету. Це дозволяє використовувати його в середовищах з високими вимогами до інформаційної безпеки, таких як розвідка, оборонна аналітика або архівна криміналістика. Завдяки своїй модульній структурі програма може бути легко адаптована до конкретних потреб користувача, включаючи можливість інтеграції з новими алгоритмами цифрової обробки [41].

Загалом, за результатами тестування, вдосконалена версія PixelProfile демонструє високу ефективність у верифікації цифрових зображень, підтверджує свою надійність у виявленні маніпуляцій та має значний потенціал для подальшого використання у прикладних та наукових дослідженнях.

# ВИСНОВКИ

У ході виконання дипломної роботи мною було розроблено, вдосконалено та протестоване програмне забезпечення PixelProfile, що призначене для аналізу цифрових зображень з метою виявлення їх модифікацій, зокрема в супутникових та аерофотознімків. Основна мета дослідження – підвищення функціональності та адаптації інструменту до сучасних вимог цифрової криміналістики, а також забезпечення ширших можливостей інтеграції з передовими технологіями аналізу зображень. У роботі мною реалізовано перехід від застарілої платформи Delphi до сучасного середовища Java, що забезпечило кросплатформеність, покращену продуктивність, зручніший інтерфейс користувача та відкритість до подальшої інтеграції з бібліотеками машинного навчання, наприклад, такими як OpenCV.

Завдяки впровадженню нових методів аналізу – 2D-RGB, 3D-RGB, Фур'є-аналізу, а також алгоритмів виявлення підробок типу Copy-Move та сплайсингу – програма PixelProfile отримала істотне розширення свого інструментарію. Це дозволило підвищити точність і ефективність аналізу навіть без використання попередньо вбудованих маркерів або водяних знаків. Комплексне застосування спектральних, піксельних та фізичних підходів до виявлення змін також забезпечує можливість автоматизованої верифікації зображень, що є критично важливим у сучасних умовах інформаційної безпеки. Переваги переходу на платформу Java сприяли кращій інтеграції з сучасними технологіями аналізу зображень, включаючи підтримку бібліотек на основі машинного навчання та відкриття нових можливостей для масштабування. Крім того, мною було досягнуто оптимізації продуктивності, що особливо важливо при обробці великих обсягів даних та високороздільних супутникових знімків. Також значно покращено зручність користувацького інтерфейсу, що розширює коло потенційних користувачів і полегшує доступ до ключових функцій програми.

Особлива увага була приділена вдосконаленню алгоритмів виявлення прихованих редагувань на супутникових знімках, які можуть маскувати військову техніку, об’єкти інфраструктури або інші критично важливі елементи. Отримані результати свідчать про ефективність запропонованого підходу, зокрема в частині

виявлення слабко виражених слідів фальсифікації. Навіть без проведення повної кількісної оцінки ефективності, якісний порівняльний аналіз із наявними інструментами — такими як Izitru, FotoForensics та Forensically — засвідчив переваги PixelProfile у глибині спектрального аналізу та можливості адаптації до конкретних потреб аналітика. Більшість згаданих веб-сервісів орієнтовані переважно на перевірку справжності JPEG-файлів і мають обмежену функціональність при роботі з іншими форматами зображень або складними видами цифрових маніпуляцій. На відміну від них, PixelProfile забезпечує повністю офлайн-середовище для роботи, що є критично важливим в умовах обмеженого або закритого доступу до мережі — наприклад, у військовій сфері, де безпека даних і автономність програмного забезпечення мають першорядне значення.

Очевидною є народногосподарська та прикладна значущість розробки, особливо в умовах сучасних викликів у сфері інформаційної безпеки та геоінформаційних технологій. Використання програми у військовій розвідці, моніторингу територій, аналізі супутникових змін для цілей безпеки або гуманітарного реагування є найбільш пріоритетними напрямками її застосування. Завдяки своїй відкритості, гнучкості та науковій обґрунтованості, розробка має потенціал для впровадження в практичну діяльність як державних, так і приватних структур, що працюють у сфері ДЗЗ, геоаналітики, безпеки та журналістських розслідувань.

Наукова значущість роботи полягає у міждисциплінарному підході до проблеми – поєднанні знань із цифрової обробки сигналів, комп’ютерного зору, методів спектрального аналізу та криміналістики з практичним програмуванням і системним інжинірингом. У результаті проведеного дослідження розширено теоретичну базу методів виявлення цифрових маніпуляцій, а також запропоновано реальні приклади їх реалізації у вигляді працюючого програмного забезпечення. Запланована публікація статті на основі матеріалів дипломної роботи підтверджує наукову новизну та актуальність проведеного дослідження.

Подальші дослідження в межах проєкту PixelProfile доцільно зосередити на кількох ключових напрямах. Насамперед, перспективним є впровадження модулів штучного інтелекту, зокрема згорткових нейронних мереж (CNN) для

автоматичного виявлення аномалій у цифрових зображеннях. Інтеграція таких алгоритмів дозволить значно підвищити точність і автономність аналізу, особливо при роботі з великими наборами супутникових та аерофотознімків. Важливою задачею також залишається повна автоматизація процесів аналізу — від завантаження зображення до генерації звіту про підозрілі ділянки. Створення веб-інтерфейсу або хмарного сервісу, здатного обробляти дані у реальному часі, зробить інструмент зручнішим для широкого кола користувачів, зокрема у сфері розвідки, екологічного моніторингу чи журналістських розслідувань. Окремо слід відзначити необхідність подальшої роботи над методами спектрального аналізу, зокрема Фур'є-аналізом. Як показало дослідження, цей метод, попри свою теоретичну цінність, виявився малоефективним у практичному застосуванні для виявлення змін у зображеннях. Основна проблема полягає в складності інтерпретації спектральних даних людиною, а також у недостатній локалізації змінених ділянок. У майбутньому важливо вдосконалити візуалізацію результатів Фур'є-аналізу, автоматизувати виявлення характерних частотних аномалій і поєднати цей метод із іншими — наприклад, з аналізом різкості або колірної структури — для підвищення його ефективності.

Таким чином, результати дипломної роботи мають практичну, наукову та соціальну цінність. Розроблені підходи і програмні рішення можуть стати основою для подальших досліджень, розробок і впровадження в реальні проєкти, що спрямовані на забезпечення достовірності цифрових зображень, боротьбу з дезінформацією та захист критичної інформаційної інфраструктури.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ding S., Ni Y., Yao J., Tan J., Lan Y. Forensic research of satellite images forgery: a comprehensive survey [Електронний ресурс] // Artificial Intelligence Review. – 2024. – Vol. 57, No. 9. – Article No. 253. – Режим доступу: https://link.springer.com/article/10.1007/s10462-024-10909-w (дата звернення: 13.05.2025).

2. Gonzalez R. C., Woods R. E. Digital Image Processing. 4th ed. London : Pearson Education, 2018. 1024 p.

3. Farid H. Photo Forensics. Cambridge (MA) : MIT Press, 2016. 323 p.

4. Sharma, V., Jha, S., & Bharti, R. K. (2016). Image Forgery and it’s Detection Technique: A Review. International Research Journal of Engineering and Technology (IRJET), 3(3), 756–762.

5. Sharma P., Kumar M., Sharma H. Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation // Multimedia Tools and Applications. — 2022. — Vol. 82, No. 12. — P. 18117–18150. — Режим доступу: 10.1007/s11042-022-13808-w.

6. Abedi F., Rajabifard A. Ethics, privacy and the perils of 'deepfake geography' [Електронний ресурс] // Pursuit. — 2024. — 25 верес. — Режим доступу: https://pursuit.unimelb.edu.au/articles/ethics-privacy-and-the-perils-of-deepfake-geography (дата звернення: 18.04.2025).

7. Lin E. T., Podilchuk C. I., Delp E. J. Detection of image alterations using semifragile watermarks // Security and Watermarking of Multimedia Contents II : Proc. SPIE. — 2000. — Vol. 3971. — P. 152–163.

8. Ansari M. D., Ghrera S. P., Tyagi V. Pixel-Based Image Forgery Detection: A Review // IETE Journal of Education. — 2014. — Vol. 55, No. 1. — P. 40–46.

9. Correct File Formats: RGB and CMYK [Електронний ресурс] // Vistaprint Hub. — Режим доступу: https://www.vistaprint.com/hub/correct-file-formats-rgb-and-cmyk (дата звернення: 16.05.2025).

10. MIL-STD-2500C. Department of Defense Interface Standard: National Imagery Transmission Format (Version 2.1). Washington, D.C. : Department of Defense, 2006. 159 p.

11. Jensen J. R. Introductory Digital Image Processing: A Remote Sensing Perspective. 4th ed. Upper Saddle River (NJ) : Pearson Education, 2015. 544 p.

12. OpenCV (Open Source Computer Vision Library) [Електронний ресурс]. — Режим доступу: https://opencv.org (дата звернення: 14.04.2025).

13. Ferreira W. D., Ferreira C. B. R., da Cruz Júnior G., Soares F. A review of digital image forensics // Computers & Electrical Engineering. — 2020. — Vol. 85. — Article 106685.

14. Algorithms for Encrypting Images using SEE Transformation [Електронний ресурс] / Mohamed Yahay, Najlae Falah Hameed Al Saffar // International Journal for Research Trends and Innovation. — 2023. — Vol. 8, Issue 4. — Article IJRTI2304091. — С. 536. — Режим доступу: https://www.ijrti.org (дата звернення: 18.04.2025).

15. Roy A., Dixit R., Naskar R., Chakraborty R. S. Digital Image Forensics: Theory and Implementation. Singapore : Springer, 2019. 105 p.

16. Is This North Korean Hovercraft Landing Photo Faked? [Електронний ресурс] // The Atlantic. — Режим доступу: https://www.theatlantic.com/photo/2013/03/is-this-north-korean-hovercraft-landing-photo-faked/100480/ (дата звернення: 18.04.2025).

17. Sial H. A., Baldrich R., Vanrell M., Samaras D. Light Direction and Color Estimation from Single Image with Deep Regression [Електронний ресурс] // arXiv. — 2020. — Режим доступу: https://arxiv.org/abs/2009.08941 (дата звернення: 18.04.2025).

18. JEITA CP-3451C (CIPA DC-008-2012). Exchangeable Image File Format for Digital Still Cameras: Exif Version 2.3. Tokyo: Japan Electronics and Information Technology Industries Association, 2012. 191 p.

19. Melvin C. Real or fake? Izitru uses forensic analysis to spot bogus images [Електронний ресурс] // Digital Trends. — 2014. — 12 трав. — Режим доступу: https://www.digitaltrends.com/photography/izitru-service-spots-bogus-images-using-forensics/ (дата звернення: 13.04.2025).

20. FotoForensics [Електронний ресурс]. — Режим доступу: https://fotoforensics.com (дата звернення: 13.04.2025).

21. Tommy Built UMP: brace or SBR? [Електронний ресурс] // HKPRO Forums. — Режим доступу: https://www.hkpro.com/threads/tommy-built-ump-brace-or-sbr.541784/ (дата звернення: 18.04.2025).

22. Forensically: free online photo forensics tools [Електронний ресурс] / Jonas Wagner. — Режим доступу: https://29a.ch/photo-forensics (дата звернення: 13.04.2025).

23. Delphi – IDE Software Overview [Електронний ресурс] // Embarcadero Technologies. — Режим доступу: https://www.embarcadero.com/products/delphi (дата звернення: 14.04.2025).

24. How does Delphi compare to Java for enterprise applications? [Електронний ресурс] // Lemon.io Q&A. — Режим доступу: https://lemon.io/answers/delphi/how-does-delphi-compare-to-java-for-enterprise-applications/ (дата звернення: 14.04.2025).

25. Overview of Java [Електронний ресурс] // Oracle Help Center. — Режим доступу: https://docs.oracle.com/en/database/oracle/oracle-database/19/jjdev/Java-overview.html (дата звернення: 14.04.2025).

26. JavaFX – OpenJFX [Електронний ресурс] : офіційний сайт проєкту. — Режим доступу: https://openjfx.io/ (дата звернення: 15.04.2025).

27. JFreeChart [Електронний ресурс] : офіційний вебсайт бібліотеки. — Режим доступу: http://www.jfree.org/jfreechart/ (дата звернення: 15.04.2025).

28. Colantoni P., Trémeau A. 3D Visualization of Color Data to Analyze Color Images // Proc. of the PICS Conference (Rochester, USA). — 2003. — C. 500–505.

29. Burger W., Burge M. Digital Image Processing: An Algorithmic Introduction Using Java. 2nd ed. London : Springer, 2016. 811 c. — (Texts in Computer Science).

30. Fridrich J., Soukal D., Lukáš J. Detection of Copy-Move Forgery in Digital Images // Proc. of the Digital Forensic Research Workshop (DFRWS). — Cleveland, OH, USA, August 5–8, 2003. — P. 19–23.

31. Fang Z., Wang S., Zhang X. Image Splicing Detection Using Color Edge Inconsistency // Proc. of the 2010 International Conference on Multimedia Information Networking and Security (MINES). — 2010. — P. 923–926.

32. Lukáš J., Fridrich J., Goljan M. Detecting Digital Image Forgeries Using Sensor Pattern Noise // Proc. SPIE: Security, Steganography, and Watermarking of Multimedia Contents VIII. — 2006. — Vol. 6072. — P. 60720Y-1–60720Y-11.

33. Карта місцевості (скріншот із сервісу Google Earth) [Електронний ресурс]. — Режим доступу: https://earth.google.com/web/?hl=uk (дата звернення: 18.04.2025).

34. Ding S., Ni Y., Yao J., Tan J., Lan Y. Forensic research of satellite images forgery: a comprehensive survey [Електронний ресурс] // Artificial Intelligence Review. – 2024. – Vol. 57, No. 9. – Article No. 253. – Режим доступу: https://link.springer.com/article/10.1007/s10462-024-10909-w (дата звернення: 13.05.2025).

35. Compton L. JPEGsnoop – JPEG Decoding & Analysis [Електронний ресурс] // DME Resources. – 2023. – Режим доступу: https://dmeresources.com/index.php/component/edocman/187-jpegsnoop-jpeg-decoding-analysis (дата звернення: 16.04.2025).

36. Tanasi A., Buoncristiano M. Ghiro – Automated Digital Image Forensics Tool [Електронний ресурс] // getghiro.org. – 2024. – Режим доступу: https://getghiro.org/ (дата звернення: 17.04.2025).

37. Horvath J., Mas M.D., Hao H., Delp E.J. Manipulation Detection in Satellite Images Using Deep Belief Networks [Тези конференції] // Proc. of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops. – 2020. – P. 664–665. – Режим доступу: https://openaccess.thecvf.com/content_CVPRW_2020/html/w39/Horvath_Manipulation_Detection_in_Satellite_Images_Using_Deep_Belief_Networks_CVPRW_2020_paper.html (дата звернення: 16.04.2025).

38. Riedlbauer D., Nitti M. E., Li L. OSINT ToolKit: FotoForensics can help uncover image manipulation during a crisis to protect against mis/disinformation [Електронний ресурс] // Counterterrorism Group. – 2024. – Режим доступу: https://www.counterterrorismgroup.com/post/osint-toolkit-fotoforensics-can-help-uncover-image-manipulation-during-a-crisis-to-protect-against (дата звернення: 16.04.2025).

39. Krawetz N. Tutorial: Error Level Analysis [Електронний ресурс] // FotoForensics. – Режим доступу: https://fotoforensics.com/tutorial-ela.php (дата звернення: 17.04.2025).

40. Cannas E.D. Forensic Analysis of Satellite Imagery: Challenges and Solutions [Електронний ресурс] // Special Topics in Information Technology / ed. S. Garatti. – Cham : Springer, 2025. – С. 101–110. – (SpringerBriefs in Applied Sciences and Technology). – Режим доступу: https://link.springer.com/chapter/10.1007/978-3-031-80268-3_10 (дата звернення: 17.04.2025).

41. Forensically Image Verification Tool [Електронний ресурс] // RAND Corporation. – 2023. – (Fighting Disinformation Project). – Режим доступу: https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/forensically-image-verification-tool.html (дата звернення: 16.04.2025).