Міністерство освіти і науки України

Державний університет «Одеська політехніка»

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Берія Давид Юрійович,

студент групи РЗ-161

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Модифікація методу виявлення підвищення різкості для цифрового зображення

(Комплексна)

Модифікація методу виявлення підвищення різкості для цифрового зображення у форматі без втрат

Спеціальність:

125 Кібербезпека

Керівник:

Зоріло Вікторія Вікторівна,

к.т.н.

Одеса – 2021

Міністерство освіти і науки України
Державний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Рівень вищої освіти другий (магістерський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

_____
д.т.н.,проф. А.А.Кобозєва
____ _____2021р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Берії Давиду Юрійовичу

1.Тема роботи: *Модифікація метода виявлення підвищення різкості для цифрового зображення (комплексна). Модифікація метода виявлення підвищення різкості для цифрового зображення у форматі без втрат.*
керівник роботи *Зоріло Вікторія Вікторівна, к. т. н.,*
затверджені наказом ректора університету від „25” жовтня 2021 р. № 372-в.
2.Зміст роботи*: огляд підходів та методів вирішення проблеми виявлення порушень цілісності цифрового зображення, модифікація методу виявлення штучного підвищення різкості, реалізація модифікованого методу.*
3. Перелік ілюстративного матеріалу: *слайди презентації*.

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

6. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*01.09.2021*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*15.01.2021*	*виконано*
3	*Аналіз основних аспектів виявлення підвищення різкості ЦЗ*	*01.10.2021*	*виконано*
4	*Розробка програмного забезпечення для проведення обчислювального експерименту*	*10.10.2021*	*виконано*
5	*Розробка програмного забезпечення для реалізації модифікованого методу виявлення підвищення різкості*	*17.10.2021*	*виконано*
6	*Підготовка тексту роботи*	*01.11.2021*	*виконано*
7	*Підготовка презентації та доповіді*	*12.11.2021*	*виконано*
8	*Попередній захист*	*26.11.2021*	*виконано*
9	*Нормоконтроль, рецензування*	*15.12.2021*	*виконано*
10	*Занесення роботи в електронний архів*	*18.12.2021*	*виконано*
11	*Допуск до захисту у завідувача кафедри*	*19.12.2021*	*виконано*

Здобувач вищої освіти _____ *Берія Д.Ю.*

Керівник роботи _____ *Зоріло В.В.*

ЗАВДАННЯ

на розробку розділу «Охорона праці»

Берії Давиду Юрійовичу, група РЗ-161

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Тема роботи *Модифікація метода виявлення підвищення різкості для цифрового зображення (комплексна). Модифікація метода виявлення підвищення різкості для цифрового зображення у форматі без втрат.*

Зміст розділу:

1. Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів.
2. Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях.
3. Проектування системи освітлення.

Керівник роботи

_____ (В.В. Зоріло)

«____» _____ 2021 р.

Консультант з охорони праці

_____ (_____)

«____» _____ 2021 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему «*Модифікація метода виявлення підвищення різкості для цифрового зображення (комплексна). Модифікація метода виявлення підвищення різкості для цифрового зображення у форматі без втрат*» на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 – Кібербезпека містить 18 рисунків, 7 таблиць, 33 літературних джерел за переліком посилань. Робота виконана на 55 сторінках загального тексту і 43 сторінках основного тексту.

Метою роботи є підвищення ефективності виявлення обробки цифрового зображення шляхом розробки методу.

У роботі проведено аналіз параметрів цифрового зображення, що дозволило виконати модифікацію методу виявлення штучного підвищення різкості цифрових зображень.

У результаті виконання кваліфікаційної роботи модифіковано та реалізовано метод виявлення штучного підвищення різкості цифрових зображень. При тестуванні методу кількість помилок першого роду склала 4%, другого роду – 7%.

ЦИФРОВЕ ЗОБРАЖЕННЯ, ПІДВИЩЕННЯ РІЗКОСТІ, ФАЛЬСИФІКАЦІЯ, ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ.

ABSTRACT

Qualification work on the topic «Modification of the method of detecting sharpening for digital images (complex). Modification of the method of detecting sharpening for digital image in lossless format» for the second (master's) level of higher education in the specialty 125 – Cybersecurity contains 18 figures, 7 tables, 33 references at the list of references. The work is performed on 55 pages of general text and 43 pages of main text.

The aim of the work is to increase the efficiency of digital image processing detection by developing a method.

The paper analyzes the parameters of the digital image, which allowed to modify the method of detecting artificial sharpening of digital images.

As a result of the qualification work, the method of detecting artificial sharpening of digital images was modified and implemented. When testing the method, the number of errors of the first kind was 4%, the second kind - 7%.

DIGITAL IMAGE, SHARPENING, FALSIFICATION, DETECTION OF INTEGRITY VIOLATIONS.

ЗМІСТ

ВСТУП

Маніпуляції із зображеннями знизили нашу довіру до цифрових зображень. Метод підробок стають все витонченішими та візуально не помітнішими. В епоху цифрових технологій наявність потужного і безкоштовного програмного забезпечення для редагування зображень означає, що створення візуально переконливих фотопідробок зростає з неймовірною швидкістю. Зростання маніпуляцій із фотографіями має наслідки майже у всіх сферах – від правоохоронних органів та національної безпеки до наукових видань, політики, засобів масової інформації та реклами. Важливість цього питання стає очевидною, якщо врахувати, що частіше за все в сучасному суспільстві ми все ще покладаємось на людей, які судять про достовірність зображення. Це поширюється майже на всі цифрові зображення, від тих, які використовуються як докази в залі суду, до тих, які ми бачимо щодня в газетах та журналах. Необхідна впевненість в тому, що у використовувані тут цифрові зображення, не були внесені будь-які зміни. А так як завдання виявлення фальсифікації цифрових зображень все ще не було ефективно вирішено, то це залишає його актуальним на сьогоднішній день.

Метою роботи є підвищення ефективності виявлення обробки цифрового зображення шляхом розробки методу.

Об’єктом дослідження є процес виявлення фальсифікації цифрового зображення.

Предметом дослідження є методи та засоби вирішення задачі процесу виявлення фальсифікації цифрового зображення.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз доступних джерел з виявлення порушень цілісності цифрових зображень;

– визначити параметри цифрового зображення для аналізу;

– провести обчислювальний експеримент з використанням зображень, оброблених фільтром фоторедактору GIMP «Unsharp Mask»;

– модифікувати і реалізувати алгоритм методу виявлення штучного підвищення різкості.

Практичне значення одержаних результатів. Результатом роботи є модифікований метод виявлення штучного підвищення різкості цифрового зображення у форматі без втрат та програмний продукт, що реалізовує цей метод. Програмний продукт може бути використаний для доповнення комплексної системи виявлення порушення цілісності цифрових зображень. Результати роботи опубліковано у фаховому науковому журналі «Інформатика та математичні методи в моделюванні» [1].

1 ОГЛЯД ПІДХОДІВ ТА МЕТОДІВ ВИРІШЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

Глобальна інформатизація сучасного суспільства тягне за собою використання цифрових сигналів, зокрема, цифрових зображень (ЦЗ) у різних сферах діяльності людини: судові справи, медицина, наука, мистецтво.

Стрімкий розвиток IT-технологій, здешевлення та загальнодоступність редагуючих цифрові сигнали програмних засобів, таких як, наприклад, Adobe Photoshop або GIMP, призводить до росту комп'ютерної злочинності, зокрема, до значного збільшення випадків несанкціонованих змін ЦЗ.

Так як існує багато способів зміни стану ЦЗ, що відрізняються за своєю суттю і спрямованістю, існує й безліч методів виявлення наслідків впливу на них чи порушення їх цілісності.

Дані обставини зумовлюють необхідність постійного розвитку та удосконалення методів захисту інформації.

Для всебічного вирішення питань інформаційної безпеки ефективною є комплексна система захисту інформації (КСЗІ), що поєднує в собі наступні заходи [2]: законодавчі, морально-етичні, фізичні, адміністративні, технічні, криптографічні та програмні .

Всі методи захисту інформації можна розділити на методи активного захисту (МАЗІ), спрямовані на запобігання несанкціонованого доступу, витоку, зміни інформації, і методи пасивного захисту інформації (МПЗІ), призначені для того, щоб визначити, чи було зроблено навмисне порушення цілісності інформації [3].

Методи активного захисту за способом їх реалізації поділяють на програмні, криптографічні, технічні та організаційні. МПЗІ в свою чергу поділяють за способом їх реалізації на методи експертної оцінки, програмно-технічні та програмні.

Програмно-технічні МПЗІ грунтуються на знаннях та аналізі специфічних особливостей пристроїв аудіо-, відео- або фотофіксації та (або) впливу будь-яких зовнішніх факторів на проведення запису.

Під час аналізу цілісності ЦЗ методи експертної оцінки полягають у тому, що експерт за допомогою візуального аналізу намагається виявити прості геометричні невідповідності в падінні/відображенні світла/тіні, а також всілякі викривлення перспективи [4]. Наявність слідів ретуші, невідповідність колірних тонів в околиці контуру підозрілого об'єкта, порушення пропорцій також вказує на порушення цілісності графічної інформації. Головним недоліком методів експертної оцінки є наявність людського фактора. Суб'єктивна оцінка – це важкий і повільний процес, який вимагає досвідчених експертів і не є об'єктивним і універсальним.

Один з найбільш ефективних програмно -технічних методів захисту ЦЗ від несанкціонованих змін заснований на аналізі вбудованого в об'єкт, що захищається, цифрового водяного знаку (ЦВЗ) [5-10]. Розробки в цій галузі ведуть спеціалісти в усьому світі. На відміну від звичайних водяних знаків ЦВЗ можуть бути не тільки видимими, але і (як правило) невидимими. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або керуючу інформацію [5]. Задачу вбудовування (здійснюваного МАЗІ) та аналізу ЦВЗ (здійснюваного МПЗІ) виконує стегосистема. У більшості стегосистем для впровадження та виділення ЦВЗ використовується ключ. Ключ може бути призначений для вузького кола осіб або ж бути загальнодоступним. Якщо ЦВЗ використовується для підтвердження автентичності, то неприпустимі зміни контейнера (ЦЗ) повинні призводити до руйнування ЦВЗ, що і буде зафіксовано МПЗІ при його аналізі. Але метод з використанням ЦВЗ не позбавлений серйозних недоліків. У порушника на законних підставах може матися декодер – пристрій виявлення ЦВЗ (наприклад, у складі DVD-програвача), а також йому може бути відомий ключ, тоді не важко витягти ЦВЗ із зображення, внаслідок чого при фальсифікації зображення не викличе ніяких підозр. Ще один мінус цього

способу полягає в тому, що ЦВЗ повинен бути занурений в цифровий об'єкт безпосередньо під час створення цього об'єкта, що обмежує область застосування методу тільки для механізмів генерації ЦЗ, що мають вбудовані можливості занурення ЦВЗ, чого більша частина широко використовуваних фотоапаратів на сьогоднішній день немає.

Широке поширення сьогодні набули методи, засновані на аналізі EXIF-даних – додаткової інформації, що додається в медіафайли цифровою технікою безпосередньо при їх створенні [5]. За допомогою EXIF-даних можна встановити умови і способи отримання медіафайлу, авторство, координати місця зйомки (за наявності вбудованого приймача GPS) і т.д. Додаткова обробка в графічному редакторі також вносить в оброблюваний файл інформацію, що ідентифікує конкретний редактор, наявність якої в EXIF-даних побічно буде вказувати на порушення цілісності файлу. Недоліки цих методів полягають у тому, що, по-перше, існує програмне забезпечення для зміни EXIF-даних з метою виправлення автоматично зміненої в процесі обробки файлу інформації, по-друге, дані методи дозволяють зробити висновок про можливе редагування файлу, але не визначають область і характер редагування, що не дає можливості використання їх для достовірного дослідження ЦЗ на порушення цілісності.

Основним недоліком програмно-технічних методів захисту інформації є жорстка прив'язаність до технічного пристрою, його можливостей і властивостей або впливу оточуючих факторів на запис сигналу. Крім того в більшості випадків при виявленні фальсифікації дані методи не здатні локалізувати її область.

На відміну від програмно-технічних і експертних методів програмні методи не мають прив'язки до технічних пристроїв, за допомогою яких було отримано інформацію, а також зазвичай не вимагають участі експерта в ідентифікації порушень її цілісності.

Неможливо гарантувати абсолютну успішність МАЗІ в будь-якій системі захисту інформації, що робить МПЗІ обов'язковою складовою

частиною комплексної системи захисту інформації; крім того, якщо несанкціоновані зміни інформаційного контенту відбулися поза розглянутої інформаційної системи, вони принципово не можуть бути попереджені МАЗІ, а можуть бути виявлені тільки за допомогою МПЗІ, що визначає важливість, потребу і значимість цієї категорії методів в абсолютному значенні.

На даний час активно розвивається галузь експертизи цифрових контентів, створюються нові та вдосконалюються існуючі програмні методи виявлення порушень цілісності ЦЗ, таких як клонування (заміна частини основного зображення замінюється частиною цього ж зображення) [11-15], колаж (комбінація частин різних зображень) [16], масштабування (зміна розмірів та (або) поворот частин ЦЗ) [17-18], корекція яскравості [19], постобробка ЦЗ після його фальсифікації (ретуш, зміна різкості, регулювання контрасту, підвищення різкості, розмиття).

Під порушенням цілісності у даній роботі будемо розуміти несанкціоновану зміну ЦЗ. Як показує практика, при здійснені клонування та/або колажу для приховання їх слідів часто виникає потреба у використанні такого інструменту, як розмиття. Крім того, часто розмиття застосовується у якості стеганографічної атаки на ЦЗ. Під стеганографічною атакою будемо розуміти спробу виявити, витягти, змінити приховане стеганографічне повідомлення.

І в тому, і в іншому випадку розмиття має бути настільки великим, щоб досягти мети, і настільки малим, щоб якість (чіткість) ЦЗ не викликала сумнівів в його автентичності. З врахуванням цього для обробки фальсифікованого зображення часто використовують розмиття за Гаусом.

Таким чином, наявність слідів розмиття є вказівкою на можливу фальсифікацію ЦЗ або свідчить про застосування стеганографічної атаки на піддослідне зображення. Під фальсифікацією (фотомонтажем) будемо розуміти заміну частини (частин) одного ЦЗ частиною (частинами) іншого (цього ж) ЦЗ.

На даний момент методи виявлення розмиття, про які відомо з відкритих джерел, дозволяють частково вирішити дану проблему.

В [20] представлений метод, основою якого є аналіз найбільш контрастного рядка (стовпця) зображення. Даний метод дозволяє оцінити ступінь розмиття цифрового монохроматичного напівтонового зображення. Але недоліком цього методу є те, що для оцінки ступеня розмиття потрібна попередня обробка ЦЗ. Крім цього застосування методу є можливим лише тоді, коли факт розмиття заздалегідь відомий. Метод орієнтовано не на виявлення самого розмиття, а на встановлення ступеня його розмиття, тобто визначення параметрів відповідного фільтру.

Активно протягом останнього десятиріччя розвиваються методи виявлення порушень цілісності цифрових зображень [21-25], засновані на Загальному підході до аналізу стану та технології функціонування інформаційної системи (ЗПАІС), який у свою чергу базується на матричному аналізі та теорії збурень. Головні положення ЗПАІС у контексті ЦЗ коротко описані далі.

В якості математичної моделі ЦЗ можна використовувати матрицю (скінчену множину матриць). Властивості ЦЗ, незалежно від його конкретного виду, будуть визначатися математичними властивостями відповідних матриць.

Оскільки будь-яка матриця однозначно визначається своїм сингулярним спектром – множиною сингулярних чисел (СНЧ) і набором сингулярних векторів (СНВ) спеціального виду, які можна отримати за допомогою нормального сингулярного розкладання матриці (SVD) [24], то при вибраному матричному способі формалізації цифрове зображення визначається сингулярним спектром (спектрами) і набором (наборами) СНВ відповідної йому матриці (матриць): СНЧ і СНВ несуть в собі всю інформацію про стан ЦЗ.

Довільне перетворення ЦЗ, в тому числі і фальсифікація, представляється у вигляді збурення відповідної матриці (матриць) [27],

звідки випливає, що будь-яке перетворення ЦЗ формально представляється у вигляді сукупності збурень СНЧ і СНВ відповідної йому матриці (матриць).

Як показав огляд доступних літературних джерел та інтернет-ресурсів, найчастіше при несанкціонованих змінах та постобробці після фальсифікації ЦЗ використовується розмиття зображення засобами графічних редакторів. Задача виявлення результатів дії розмиття у повній мірі не вирішена.

Як показує практика і факти, відомі з відкритої преси розмиття використовується при проведенні фотомонтажу для його приховання так, щоб візуально його якість залишалася прийнятною. Математично, фільтр Гауса являє собою згортку вхідного сигналу та функції Гауса. Це перетворення також відоме як перетворення Вейерштраса.

Фільтр Гауса зазвичай використовується в цифровому вигляді для обробки двовимірних сигналів з метою зниження рівня шуму. Візуально даний ефект являє собою легке розмиття, як при спостереженні через каламутне скло. Однією з характеристик розмиття за Гаусом є радіус розмиття, що вимірюється у пікселях. Чим він більший, тим сильніше розмиття. Значення радіусу в програмному середовищі Adobe Photoshop можна обрати від 0,1 до 250. В [26] було проведено адаптацію стеганоаналітичного методу (CAM), основою якого є теорія збурень та матричний аналіз, для задачі знаходження порушень цілісності ЦЗ, а саме накладення шуму та розмиття зображення.

Даний метод дозволяє з високою ймовірністю визначити факт порушення цілісності ЦЗ. Та недоліком цього методу є те, що він недієздатний в умовах, коли ЦЗ було збережено з втратами.

Адаптований для вирішення даної задачі CAM дозволяє з високою долею ймовірності вірно відокремити розмиті ЦЗ від нерозмитих за умови, що радіус розмиття не менше за 2 і зображення до розмиття зберігалося у форматі з втратами, а після – у форматі без втрат: кількість нерозпізнаних розмитих ЦЗ становить два відсотки.

В [25] визначені та теоретично обґрунтовані якісні характерні

особливості математичних параметрів, що визначають ЦЗ – сингулярних чисел, – які вказують на його розмиття. Матриця ЦЗ аналізується блоками розміром 8×8. Для кожного блоку знаходиться множина СНЧ, яка буде дорівнювати восьми. Для аналізу обрано найменші п'ять СНЧ через їх найбільшу відповідність високочастотній складовій сигналу ЦЗ (контурам ЦЗ), реакція яких на розмиття зображення проявляється у наступному: швидкість росту зазначених СНЧ відповідного блоку близька до нуля (при їх лінійній апроксимації) для розмитого ЦЗ на відміну від аналогічної характеристики нерозмитого ЦЗ. З ростом радіуса розмиття особливості математичних параметрів розмиття ЦЗ лише посилюються, тобто швидкість росту аналізованих СНЧ зменшується. Продовження даного дослідження знайшло своє відображення у [25], де розроблено метод відбору розмитих ЦЗ від нерозмитих. У проведеному дослідженні ЦЗ у форматі з втратами розглядаються із різним параметром якості, який далі позначається Q та приймає значення 0, 1, 2, ..., 12 згідно стандартів графічного редактору Adobe Photoshop. Даний параметр якості характеризує ступінь стиску ЦЗ у форматі JPEG. Чим вище Q, тим менше стиск і краще якість ЦЗ. Зі зменшенням Q на зображенні можлива поява артефактів стиснення, у зв'язку з чим введено обмеження за якістю: зображення з Q менше 8 не розлядаються через погану якість, яка сама по собі викликає підозри щодо автентичності ЦЗ. Розроблений у [26] метод виявлення розмиття (МВР) при додатковому дослідженні дає високу ймовірність правильних розпізнань. Даний метод є ефективним при виявленні розмиття, починаючи з радіусу один піксель, у чому полягає його головна перевага перед іншими відомими методами. Якщо розмиття ЦЗ проводиться з метою приховання результатів його фальсифікації або як стеганографічна атака, то при великому радіусі воно стає помітним візуально та одразу викликає підозри до ЦЗ.

Візуальним результатом розмиття є згладжування контурів, то даний інструмент обробки цифрового зображення призведе до зменшення

високочастотної складової сигналу, що підтверджується обчислювальним експериментом, проведеним у [27-28].

Так як візуальним результатом розмиття є згладжування контурів, то даний інструмент обробки цифрового зображення призводить до зменшення високочастотної складової сигналу. На прикладі матриці розміром 12×12 пікселів, яка є підматрецею тестового цифрового зображення, отриманого у форматі JPEG, підтверджено обов'язкове зменшення вкладу високочастотної складової цифрового зображення при його розмитті і перерозподіл енергії між іншими складовими сигналу. Однак у [27-28] зазначено, що, хоча такий перерозподіл і має місце, в цілому при розмитті його енергія, як і слід було очікувати, зменшується зі збільшенням радіусу розмиття (рис.1).

У ході обчислювального експерименту, у якому було використано 300 цифрових зображень різного формату, розміру та змісту, було встановлено, що після розмиття цифрового зображення з радіусом один піксель зменшення їх енергії відбувається в середньому на 4,8 %.

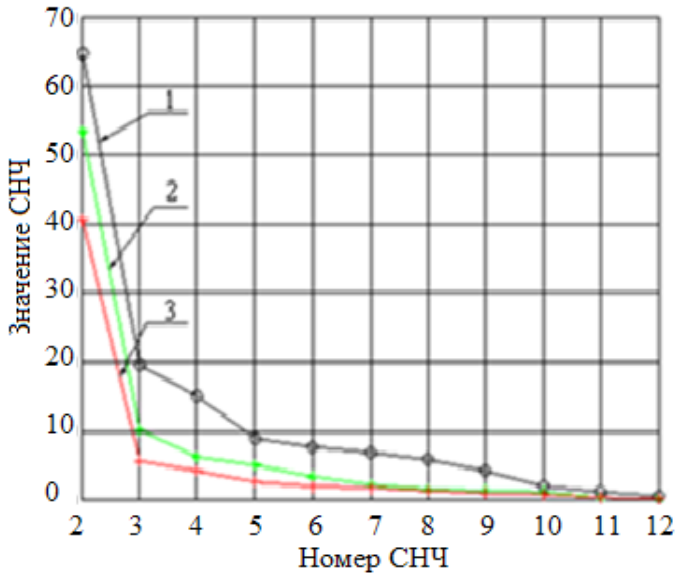


Рисунок 1 – Інтерполяційний сплайн першого степеня для множини СНЧ досліджуваного ЦЗ: 1 – вихідне ЦЗ; 2 – ЦЗ, розмите з радіусом 1; 3 – ЦЗ, розмите з радіусом 2

Після отримання кількісної оцінки використовується в методі

виявлення розмиття цифрового зображення. Як показав порівняльний аналіз методів виявлення розмиття [24], найефективнішим у даний момент є метод, заснований на ЗПАІС [24-26].

Однією з переваг даного методу є здатність відокремлювати ЦЗ, розмиті засобами графічних редакторів, від тих, які збережено у форматі з втратами з низькою якістю та (або) мають малу глибину різкості зображуваного простору. Глибина різкості зображуваного простору (ГРЗП) – це діапазон відстаней на фотографії, в якому об'єкти зйомки сприймаються різкими. Цей діапазон відстаней знаходиться навколо точки фокусування і по-іншому ще називається зоною різкості.

У першому випадку кажуть, що фотографія знята з малою глибиною різкості зображуваного простору, тому що тільки маленький діапазон відстаней навколо точки фокусування є зоною різкого відображення об'єктів зйомки.

Такі фотографії характеризуються сильним розмиттям предметів, які розташовані далеко від точки фокусування, а також велика частина кадру являє собою зону нерізкості (об'єкти знаходяться в розфокусі, розмитті).

Навпаки, коли ми можемо розрізнити різкі деталі по всій площі кадру (або на більшій частині зображення), це свідчить про велику глибину різкості. Тобто на великому діапазоні відстаней об'єкти в кадрі виглядають різкими і не розмиті.

Також метод виявлення розмиття дає можливість розпізнавання розмиття зображення, починаючи з радіуса один. Крім того, даний метод є інваріантним до стиснення, тобто залишається незмінним при тих чи інших перетвореннях, чого не можна сказати про стеганоаналітичний метод, який може бути використаний лише у разі, коли цифрове зображення після розмиття зберігається у форматі без втрат.

Як описано в [21-25], без проведення додаткової перевірки серед цифрових зображень, невірно прийнятих за розмиті, зустрічається велика кількість зображень з малою глибиною різкості зображуваного простору,

тобто коли фотографію виконано в режимі «Макрозйомка», де об’єкт чіткий, а фон навколо розмитий.

Введемо поняття експертного розмиття. Під експертним розмиттям у даній роботі будемо розуміти розмиття піддослідного ЦЗ експертом з метою встановлення/спростування первинності проведеного ним розмиття.

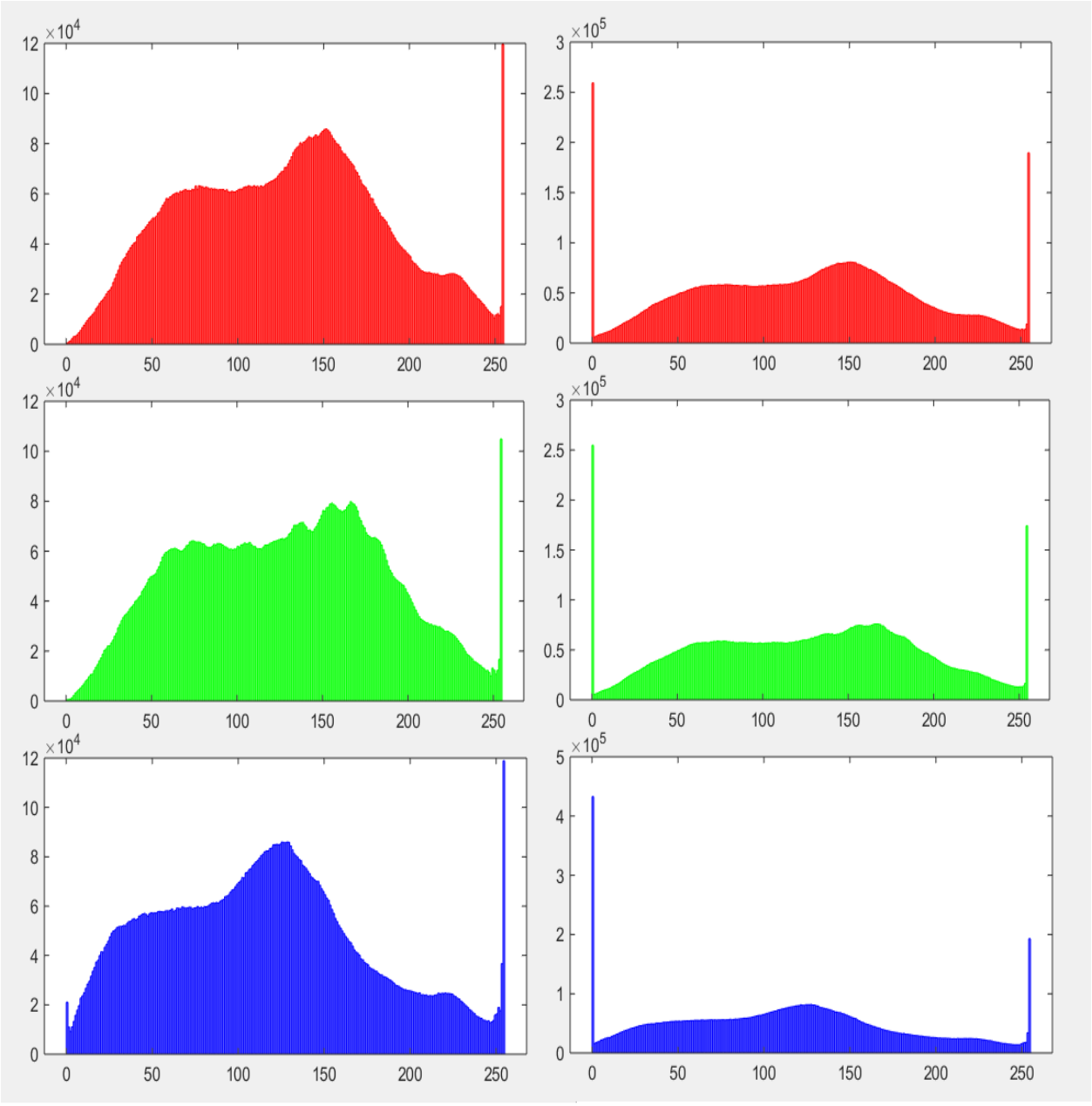
З метою відокремити розмите засобами графічних редакторів ЦЗ від зображень з малою ГРЗП у [20] проведено дослідження, яке показало, що швидкість росту відповідних СНЧ блоків матриці нерозмитого ЦЗ значно вище аналогічної характеристики для зображення, підданого розмиттю, в той час як повторне розмиття практично не змінює якісну картину у порівнянні з попереднім. Ця особливість дає можливість збільшити точність висновків про наявність навмисного розмиття засобами графічного редактору досліджуваного цифрового зображення.

Одним з програмних інструментів, який може бути використано, це штучне підвищення різкості цифрового зображення. Даний фільтр є протилежним за дією фільтру розмиття за Гаусом.

Однак виявлення його за допомогою швидкості росту сингулярних чисел ускладнюється тим, що сучасні зображення з високою ГРЗП, зроблені високоякісною фототехнікою, можуть мати таку ж високу швидкість росту відповідних сингулярних чисел, що і у зображеннях, які оброблено фільтром. Тож, доцільно шукати інший інструмент для виявлення цього виду обробки цифрового зображення.

У роботі [29] було зафіксовано ефект «піку чорного» у всіх трьох колірних компонентах матриці цифрового зображення (рис.2). Експеримент було проведено за допомогою графічного редактора GIMP, де цифрові зображення було оброблено фільтром «Unsharp mask» із параметрами за замовчуванням, що призвело до штучного підвищення різкості цифрових зображень. Після обробки зображення було збережено у форматі без втрат.

Після застосування фільтру на матрицях завжди можна було спостерігати значне підвищення кількості пікселів зі значенням 0.



а)

Рисунок 2 – Гістограма кольорових компонент RGB:

а) – до обробки; б) – після обробки

Отримано помилки першого роду в кількості 10% та помилки другого роду – 18%. Не було проведено експериментів із збереженням зображень після обробки в форматі з втратами. Тож має сенс дослідити даний ефект та модифікувати метод виявлення зазначеного порушення цілісності цифрового зображення з метою зменшення кількості помилок та підвищення ефективності виявлення порушень.

У розділі один проведено аналіз літературних джерел, доступних у відкритому друці, за темою виявлення порушень цілісності ЦЗ. Виходячи з проведеного аналізу можна зробити наступні висновки: задача доказу або виявлення порушення цілісності цифрових зображень не вирішена до кінця, переважна більшість існуючих методів виявляються недієздатними при наявності постобробки ЦЗ, у зв'язку з чим залишається актуальною розробка нових методів і алгоритмів. Особливістю проведення несанкціонованих змін цифрових зображень у даний момент є практично обов'язкове використання графічних редакторів, що не може не враховуватися при розробці методів і алгоритмів виявлення порушень цілісності ЦЗ.

Виявленню результатів постобробки фальсифікованих цифрових зображень засобами графічних редакторів приділено недостатньо уваги, що спонукає шукати нові методи вирішення даної задачі.

2 МОДИФІКАЦІЯ МЕТОДУ ВИЯВЛЕННЯ ШТУЧНОГО ПІДВИЩЕННЯ РІЗКОСТІ

2.1 Основні положення методу виявлення штучного підвищення різкості

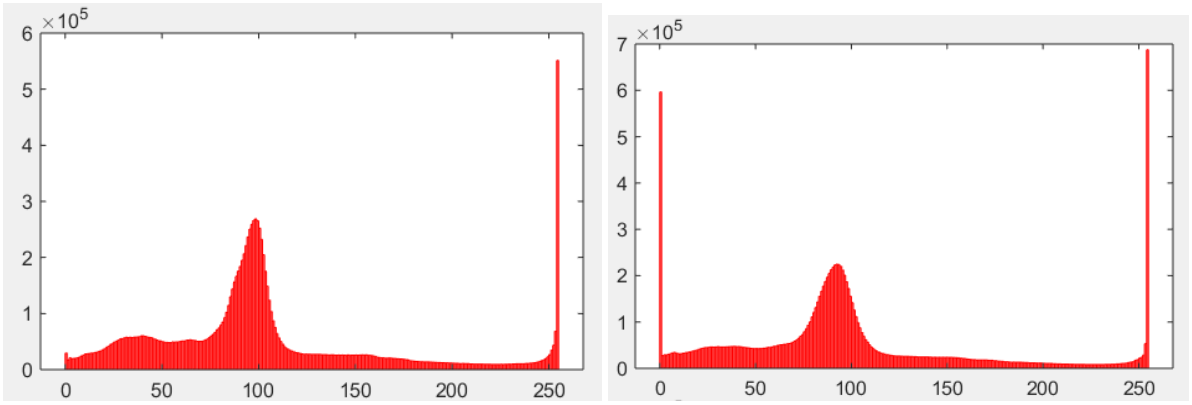
Порушення цілісності цифрових зображень не представляє складнощів для сучасних користувачів. Спеціалізоване програмне забезпечення просте й інтуїтивно зрозуміле як серед платних за стосунків (Adobe Photoshop), так і серед безкоштовних (Gimp).

Загалом усі методи підробки цифрових зображень можна поділити на дві основні категорії – зміна сцени зображення (додавання або видалення об’єктів шляхом клонування або шляхом фотомонтажу з використанням декількох зображень) та пост обробка зображення після його фальсифікації (розмиття країв доданих об’єктів, маскування розмиття підвищенням різкості, зміна кольору тощо). Штучне підвищення різкості можна використовувати як з метою приховання фотомонтажу, так і з метою стеганографічної атаки на зображення. У будь-якому випадку виявлення даного фільтру у цифровому зображенні свідчить про порушення його цілісності. Тому дана тема є актуальною.

Як зазначено в [29], при застосуванні фільтру графічного редактора Gimp «Unsharp mask» у всіх трьох колірних компонентах цифрового зображення спостерігається значне збільшення пікселів зі значенням 0. Це легко можна пояснити з урахуванням контексту вирішуваної задачі. Коли ми щось хочемо візуально виділити, то використовуємо для цього підсилення контурів темнішими кольорами. Саме це і відбувається при використанні зазначеного фільтру. Бо у діапазоні значень матриць яскравості пікселів цифрового зображення від 0 до 255 0 – найтемніший колір (чорний), 255 – найсвітліший (білий).

Візуально цей ефект дуже легко побачити при аналізі гістограм матриць яскравості цифрового зображення (рис.2.1) – чітко видно пік

гістограми саме в місці локації нульового значення. Це і є так званий «пік чорного».



а) б)

Рисунок 2.1 Гістограма компоненти R: а) – до обробки; б) – після обробки

Проте для автоматизації в роботі [29] запропоновано алгоритм, кроки якого наведемо далі.

Нехай *R*, *G* і *B* матриці червоної, зеленої та синьої компонент цифрового зображення, (r_{ij}, g_{ij}, b_{ij}) тріада цифрових компонент пікселя з координатами (i,j).

1. Для матриці *R* знайти *r*, що дорівнює кількості тріад виду $(0, g_{ij}, b_{ij})$, та знайти *r'* – кількість тріад виду $(1, g_{ij}, b_{ij})$.

Якщо $r=0$,

то вважати, що зображення необроблене фільтром «Unsharp Mask»,

інакше перейти до пункту 2.

2. Для матриці *G* знайти *g*, що дорівнює кількості тріад виду $(r_{ij}, 0, b_{ij})$, та знайти *g'*– кількість тріад виду $(r_{ij}, 1, b_{ij})$.

Якщо $g=0$,

то вважаємо, що зображення необроблене фільтром «Unsharp Mask»,

інакше перейти до пункту 3.

3. Для матриці *B* знайти *b*, що дорівнює кількості тріад виду $(r_{ij}, g_{ij}, 0)$, та знайти *b'* – кількість тріад виду $(r_{ij}, g_{ij}, 1)$.

Якщо r=0,

то вважати що зображення необробленим фільтром «Unsharp Mask»,

інакше переходимо до пункту 4.

4. *Якщо r<r'* або *g<g'* або *b<b',*

то зображення вважати необробленим фільтром «Unsharp Mask»,

інакше перейти до пункту 5.

5. Знайти коефіцієнт різкості *K* за формулою (2.1), розрахувавши попередньо відсоткові значення різниці тріад *r* та *r'* для червоної компоненти *rR* по формулі (2.2), аналогічно відсоткові значення різниці тріад g та g' для зеленої компоненти *rG* за формулою (2.3) та відсоткові значення різниці тріад *b* та *b'* для синьої компоненти *rB* за формулою (2.4):

$$K = \frac{|rR - rG| + |rG - rB| + |rB - rR|}{3}, \quad (2.1)$$

де

$$rR = \frac{(r - r') * 100}{r}, \quad (2.2)$$

$$rG = \frac{(g - g') * 100}{g}, \quad (2.3)$$

$$rB = \frac{(b - b') * 100}{b}. \quad (2.4)$$

6. *Якщо K<16,*

то будемо вважати, що зображення оброблене фільтром «Unsharp Mask»,

інакше зображення є оригінальним.

Помилки першого і другого роду при даному підході складають 10% і 18% відповідно.

Основна ідея – порівняння піку чорного з кількістю пікселів наступного за значенням кольору, тобто порівняння кількості нулів та одиниць. Якщо їх співвідношення у всіх трьох колірних компонентах менше за порогове значення, зображення вважають обробленим. В іншому випадку вважають, що штучне підвищення різкості не виявлено.

2.2 Дослідження ефекту «піку чорного» для зображень у форматі без втрат

У відкритому друці не знайдено інших робіт стосовно виявлення штучного підвищення різкості, тож немає з чим порівнювати даний метод. Проведемо дослідження даного ефекту.

Для обчислювального експерименту сформуємо базу з цифрових зображень у форматі з втратами та без втрат у кількості 600 штук: 300 з них було взято з бази NRCS [30] у форматі без втрат, та 300 цифрових зображень, отриманих сучасним сматрфоном IPhon 12 у режимі стандартної зйомки у форматі з втратами. Усі цифрові зображення було оброблено у графічному редакторі Gimp за допомогою фільтру «Unsharp mask» при стандартних параметрах фільтру. Після обробки усі цифрові зображення було збережено у форматі без втрат (bmp).

Для усіх цифрових зображень за трьома колірними компонентами було підраховано кількість пікселів зі значення 0 до та після застосування фільтру. Типові результати представлено у таблицях 2.1 – 2.3.

Таблиця 2.1

Вплив фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	25312	63526	2,50971871
2	188507	572980	3,03956882
3	954	10607	11,1184486
4	47233	162785	3,44642517
5	35054	136325	3,88899983
6	22875	109866	4,80288525
7	10696	83406	7,79786836

Таблиця 2.2

Вплив фільтру на кількість 0-пікселів зеленої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	16394	45296	2,76296206
2	82359	309015	3,75204896
3	28	4555	162,678571
4	16561	78881	4,76305779
5	8378	58510	6,98376701
6	195	38140	195,589744
7	7988	17769	2,22446169

Таблиця 2.3

Вплив фільтру на кількість 0-пікселів синьої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	2918944	3034603	1,03962358
2	240576	602991	2,50644703
3	3822	31344	8,20094192
4	1860674	1780279	0,95679254
5	3318235	3281909	0,98905261
6	775796	4783538	6,16597404
7	6233357	6285168	1,00831189

Як можемо спостерігати, результати для червоної та зеленої компонент порівняні між собою, в той час як показники синьої колірної компоненти значно відрізняються від інших двох. Отримані результати вказують на неможливість усереднення показників за трьома колірними компонентами та

використання усіх трьох компонент одночасно для виявлення зазначеного фільтру. Проте використання червоної або зеленої матриць дійсно дозволяє чітко побачити пік чорного та дає можливість використовувати цей ефект надалі.

В той самий час збільшення піку чорного також відбувається, проте не є таким вираженим при повторному застосуванні зазначеного фільтру. Для усіх оброблених зображень було проведено повторне застосування фільтру за тими ж параметрами. Результат повторної обробки збережено у форматі без втрат. Типові результати представлено у таблицях 2.4-2.6.

Таблиця 2.4

Вплив повторного застосування фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	63526	127776	2,01139691
2	572980	1070919	1,86903382
3	10607	44551	4,20015084
4	162785	331190	2,03452407
5	136325	289577	2,12416651
6	109866	247965	2,25697668
7	83406	176152	2,11198235

Як можемо бачити, дійсно при повторному застосуванні фільтра до цифрового зображення збільшення кількості пікселів зі значенням 0 у червоній колірній компоненті в більшості випадків відбувається менше, ніж у 2,25 рази в порівнянні з первинним підвищенням різкості.

Дане порогове значення визначено емпіричним шляхом. Приданому значенні кількість помилок першого роду складає 4%, помилок другого роду – 7%. Подібний результат отримано і для зеленої матриці, при використанні

зазначеного порогового значення кількість помилок першого роду 5 %, помилки другого роду – 7%.

Таблиця 2.5

Вплив повторного застосування фільтру на кількість 0-пікселів зеленої колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	45296	98576	2,1762628
2	309015	620728	2,00873097
3	4555	9618	2,1115258
4	78881	183349	2,32437469
5	58510	109870	1,87779867
6	38140	69391	1,81937598
7	17769	82912	4,66610389

Таблиця 2.6

Вплив повторного застосування фільтру на кількість 0-пікселів червоної колірної компоненти

№ цифрового зображення	Кількість 0-пікселів до обробки (N)	Кількість 0-пікселів після обробки (M)	Відношення M/N
1	3034603	3170059	1,0446371
2	602991	1095081	1,8160818
3	31344	92368	2,9469117
4	1780279	1625188	0,9128839
5	3281909	3164033	0,9640831
6	4783538	4702879	0,9831382
7	6285168	6241724	0,9930879

Використання синьої колірної компоненти дещо відрізняється від отриманих показників за іншими двома колірними компонентами. Проте використання тільки червоної колірної компоненти вже дало кращі результати в порівнянні з методом, описаним в роботі [29].

Для зручності розташуємо відношення відповідних показників у одній таблиці для червоної колірної компоненти (табл.2.7).

Таблиця 2.7

Порівняння відношень після першої та повторної обробки

№ цифрового зображення	Відношення M/N необробленого та обробленого ЦЗ	Відношення M/N обробленого та повторно обробленого ЦЗ
1	2,50971871	2,01139691
2	3,03956882	1,86903382
3	11,1184486	4,20015084
4	3,44642517	2,03452407
5	3,88899983	2,12416651
6	4,80288525	2,25697668
7	7,79786836	2,11198235

Як показав обчислювальний експеримент, при пороговому значенні 2,25 досягається найменша кількість помилок першого і другого роду.

2.3 Модифікований метод

Ефект повторної обробки вже було використано в методі виявлення розмиття цифрового зображення, заснованому на аналізі швидкості росту відповідних сингулярних чисел. Складність виявлення порогового значення для відокремлення розмитих цифрових зображень від нерозмитих була в тому, що для різних категорій зображень порогове значення також було різним. Застосування так званого експертного розмиття призвело до

уникнення необхідності використовувати чи підлаштовувати порогове значення для різних категорій цифрових зображень.

Тобто, для виявлення штучного підвищення різкості потрібно створити копію підозрюваного зображення, застосувати до неї обробку фільтром. Для обох зображень знайти кількість 0-пікселів червоної компоненти та обчислити їх співвідношення. Якщо воно менше за порогове значення, то експертну обробку слід вважати вторинною, а підозрюване зображення першочергово обробленим, тобто не автентичним.

Інколи можлива ситуація, коли кількість 0-пікселів до обробки дорівнює нулю. Тобто матимемо ділення на нуль. Для уникнення помилки у роботі програми просто вирішити цю проблему, змінивши нуль на одиницю. Це не зменшить ефективності методу, оскільки після застосування штучного підвищення різкості кількість 0-пікселів завжди буде великою.

Отже, на основі проведених експериментів та отриманих результатів складемо алгоритм модифікованого методу виявлення штучного підвищення різкості цифрового зображення.

Нехай A – підозрюване цифрове зображення, R – матриця червоної колірної компоненти цифрового зображення.

1. Для матриці R знайти r, що дорівнює кількості нульових значень.

Якщо $r=0$,

то призначити $r=1$,

інакше перейти до пункту 2.

2. Створити копію підозрюваного зображення. Застосувати до копії обробку фільтром «Unsharp Mask» графічного редактора Gimp з використанням параметрів за замовчуванням.

3. Для копії зображення виділити матрицю R'.

4. Для матриці R' знайти r', що дорівнює кількості нульових значень матриці R'.

5. Знайти *«коефіцієнт чорного»:*

$$KoefBlack = r'/r$$

6. *KoefBlack<2,25,*

то зображення вважати обробленим фільтром «Unsharp Mask»,

інакше виявлення штучного підвищення різкості не виявлено.

Обчислювальна складність даного методу є поліноміальною та порівняна з поліномом другого ступеня, визначається шляхом повного перебору значень матриці цифрового зображення m×n та порівнянням їх з нулем.

У другому розділі проведено обчислювальний експеримент, на основі якого модифіковано метод виявлення штучного підвищення різкості та розроблено його алгоритм. Модифікований метод дав кращі результати в порівнянні з оригіналом.

3 РЕАЛІЗАЦІЯ МОДИФІКОВАНОГО МЕТОДУ

Перейдемо до реалізації алгоритму модифікованого метода. І, звичайно, необхідно визначитися з середовищем для реалізації. Одним із сучасних та потужних інструментів для роботи з великим обсягом даних, з цифровими зображеннями, з реалізованими математичними функціями, які можна напряму застосовувати до об'єктів дослідження, а не писати власноруч і не витрачати на це час – середовище MATLAB.

Також треба визначити основні компоненти інтерфейсу. Нам необхідно мати два зображення в якості вхідних даних. Тож для зручності використання програмного продукту маємо передбачити об'єкти для завантаження зображень. У MATLAB це об'єкти axis. Немає необхідності у великій кількості команд у вікні програмного додатку. Основна частина алгоритму, - підрахунок кількості 0-пікселів у цифровому зображенні до та після проведення експертного підвищення різкості, пошук їх співвідношення, порівняння його з пороговим значенням, - усе це можна реалізувати однією кнопкою, аби користувач не мав змоги заплутатись у діях та функціях програмного застосунку.

Також для зручності завантаження нових зображень та коректної роботи програми передбачимо кнопку очищення об'єктів axis від зображень. Незайвою є і кнопка виходу з застосунку, хоча дану операцію можна виконати і без неї.

Отже, інтерфейс програмного продукту представлено на рисунку 3.1. Для перевірки зручності інтерфейсу було виконане опитування контрольної фокус-групи у кількості 14 осіб віком від 18 до 65 років. Усім було дано пояснення стосовно призначення даного застосунку. Отримано поради стосовно полегшення сприйняття програмного застосунку у вигляді нумерації виконання процедур за їх порядком. Після врахування даного побажання усі 100% опитуваних впорались із перевіркою зображення.

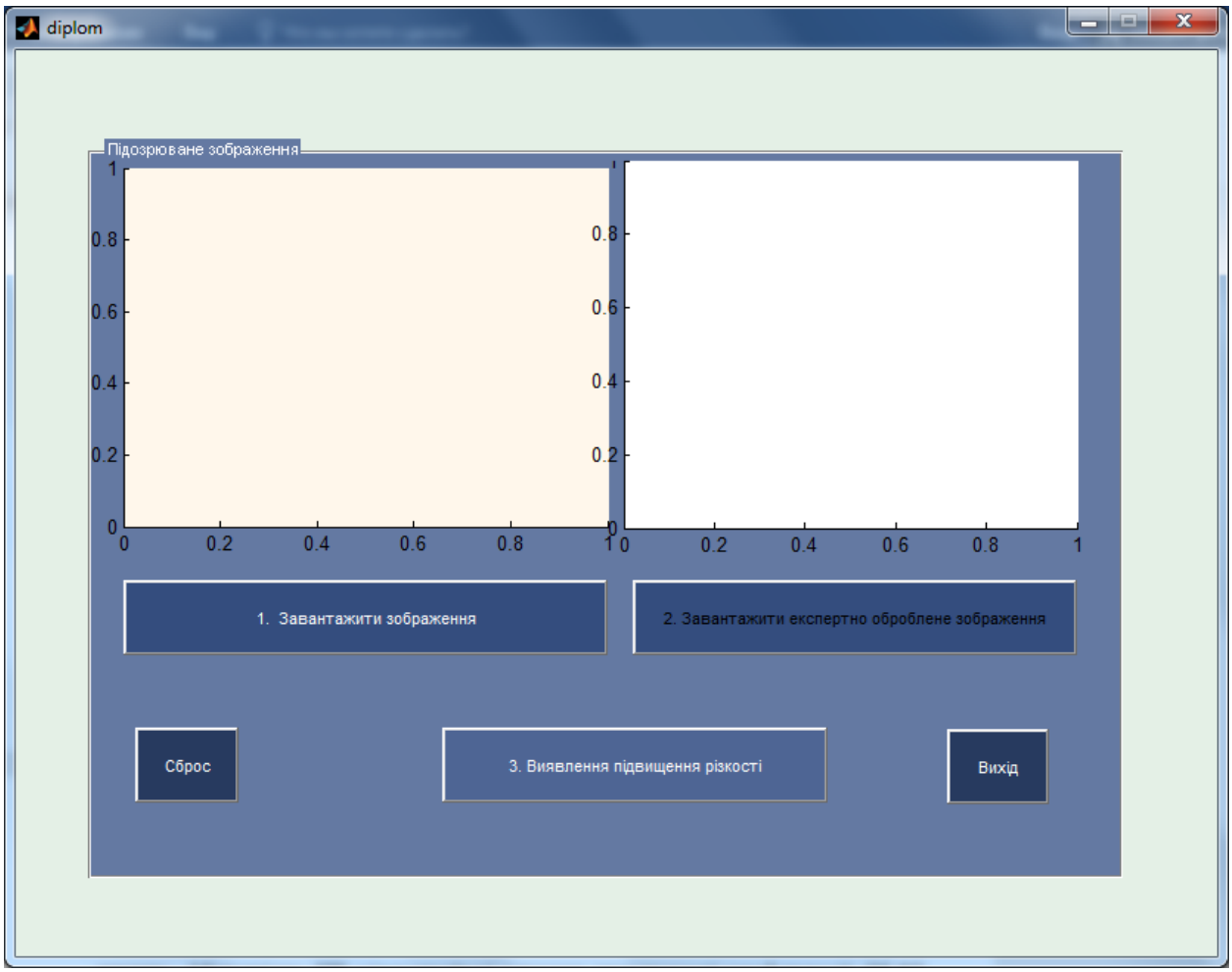


Рисунок 3.1 – Інтерфейс програмного продукту

Як бачимо, є три функціональні кнопки та дві допоміжні.

Розглянемо функціональні кнопки «Завантажити зображення» та «Завантажити експертно оброблене зображення». Програмний код для них є однаковим. Його наведено на рисунку 3.2.

Частина коду, де перелічено можливі формати цифрових зображень, наведена нижче:

```
[FileName, PathName] = uigetfile({'*.*';'*.bmp';'*.png';'*.tiff';'*.gif';...
   '*.ras';'*.jpg';'*.jpeg';},'Открыть изображение','.\Images');
```

тобто в якості вхідних даних передбачено як зображення у форматі з втратами, так і зображення у форматі без втрат.

```
36      % --- Executes on button press in pushbutton1.
37      function pushbutton1_Callback(hObject, eventdata, handles)
38 -    [FileName, PathName] = uigetfile({'*.*';'*.bmp';'*.png';'*.tiff';'*.gif';..
39          '*.ras';'*.jpg';'*.jpeg';},'Открыть изображение','.\Images');
40 -    if isequal(FileName, 0)% Если файл не был выбран
41 -        else % Если файл был выбран
42          % Формирование полного пути к файлу
43 -        FullName1 = [PathName FileName];
44          % Считывание изображения из графического файла
45 -        Pict = imread(FullName1);
46          % Вывод изображения на оси
47 -        axes(handles.axes1);
48 -        imshow (Pict);
49 -        handles.Image1 = Pict;
50 -    end
51 -    guidata(hObject, handles);
```

Рисунок 3.2 – Програмний код кнопки «Завантажити зображення».

Кнопка «Завантажити експертно оброблено зображення» має такий самий код, тож не будемо повторювати його. При натисканні кнопки 1 та кнопки 2 можемо обрати цифрове зображення для перевірки, що зберігається на внутрішніх носіях комп'ютера або на підключених до нього зовнішніх накопичувачах (рис. 3.3).

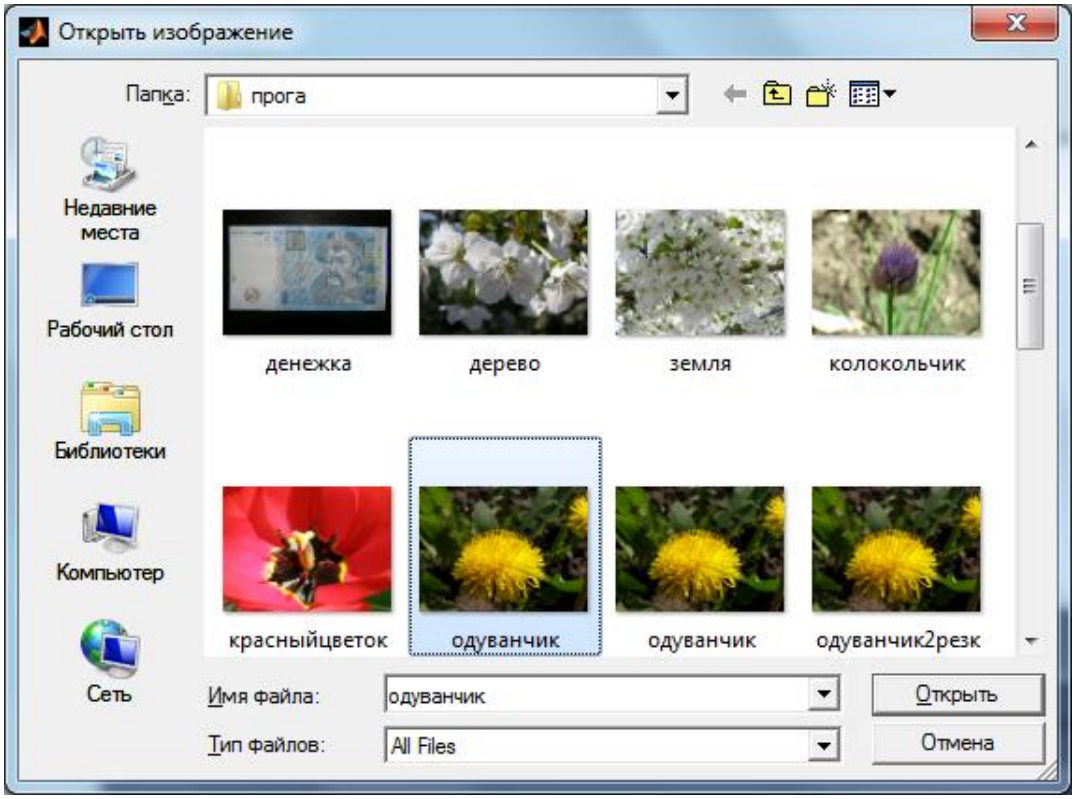


Рисунок 3.3 – Завантаження зображення для перевірки

При натисканні обох кнопок та завантаженні цифрових зображень маємо змогу побачити вибрані зображення (рис.3.4).

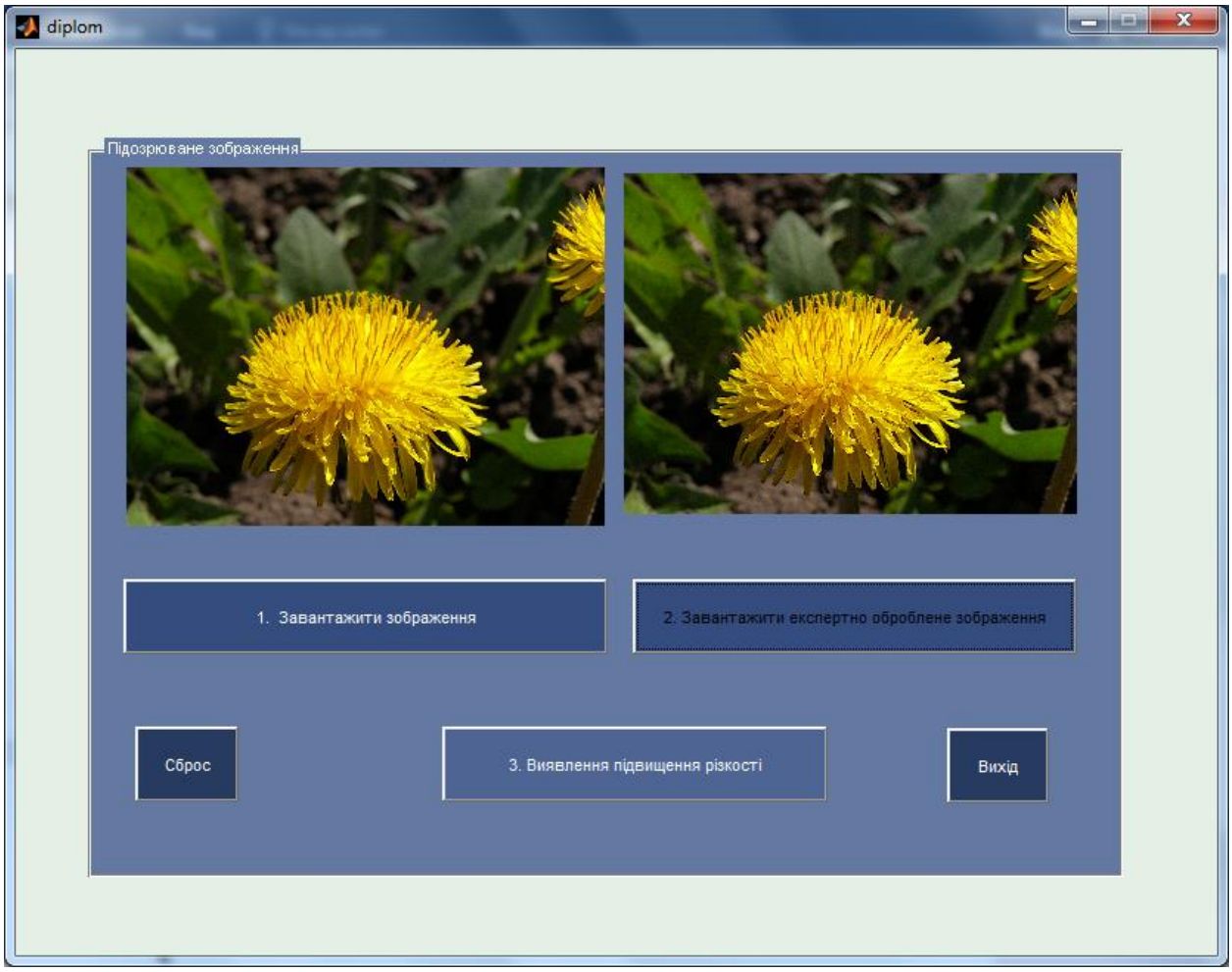


Рисунок 3.4 – Завантаження зображень для перевірки

Наступний крок – застосування кнопки 3 «Виявлення підвищення різкості». Дана кнопка містить декілька блоків програмного коду. Перший блок – перехват глобальних змінних у вигляді двох зображень для перевірки та виділення червоних колірних компонент для подальшого аналізу.

Другий блок – підрахунок кількості нульових значень у матриці підозрюваного зображення (рис.3.5). Третій блок – підрахунок кількості нульових значень матриці експертно обробленого зображення (рис.3.6). Завершальний блок – визначення співвідношення даних показників та порівняння їх з пороговим значенням (рис.3.7).

```
IZR=IZ(:,:,1);
n=fix((size(IZR,1))/8)*8;
m=fix((size(IZR,2))/8)*8;
IZR=IZR(1:n,1:m);
NulIZR=0
for i=1:n
    for j=1:m
        if IZR(i,j)==0
            NulIZR=NulIZR+1
        end
    end
end
```

Рисунок 3.5 – Підрахунок 0-пікселів підозрюваного зображення

```
IZG=IZ2(:,:,1);
l=fix((size(IZG,1))/8)*8;
k=fix((size(IZG,2))/8)*8;
IZG=IZG(1:l,1:k);
NulIZG=0
for x=1:l
    for y=1:k
        if IZG(x,y)==0
            NulIZG=NulIZG+1
        end
    end
end
```

Рисунок 3.6– Підрахунок 0-пікселів експертно обробленого зображення

```
KoefBlack=NulIZG/NulIZR;
if KoefBlack<2.25
helpdlg('Виявлено штучн  е підвищення різкості','rezult');
       else
          helpdlg('Штучне підвищення різкості не виявлено','result');
end
```

Рисунок 3.7 – Аналіз отриманих показників та висновки стосовно обробки зображення

При натисканні кнопки три виконується обробка завантажених цифрових зображень, аналіз отриманих даних. Завершальний етап роботи даної кнопки супроводжується появою вікна-повідомлення про стан

підозрюваного цифрового зображення (рис 3.8), де зазначено «Виявлено штучне підвищення різкості» або «Штучне підвищення різкості не виявлено».

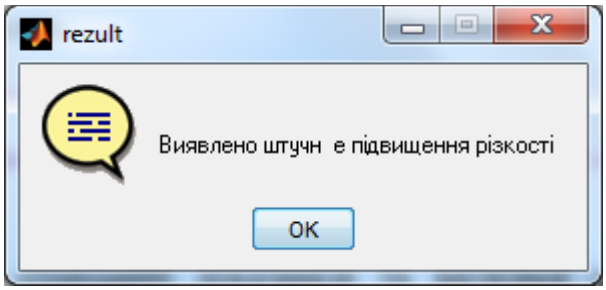


Рисунок 3.8 – Результат перевірки цифрового зображення

При натисканні кнопки «Сброс» виконується очищення об’єктів від цифрових зображень (рис 3.9).

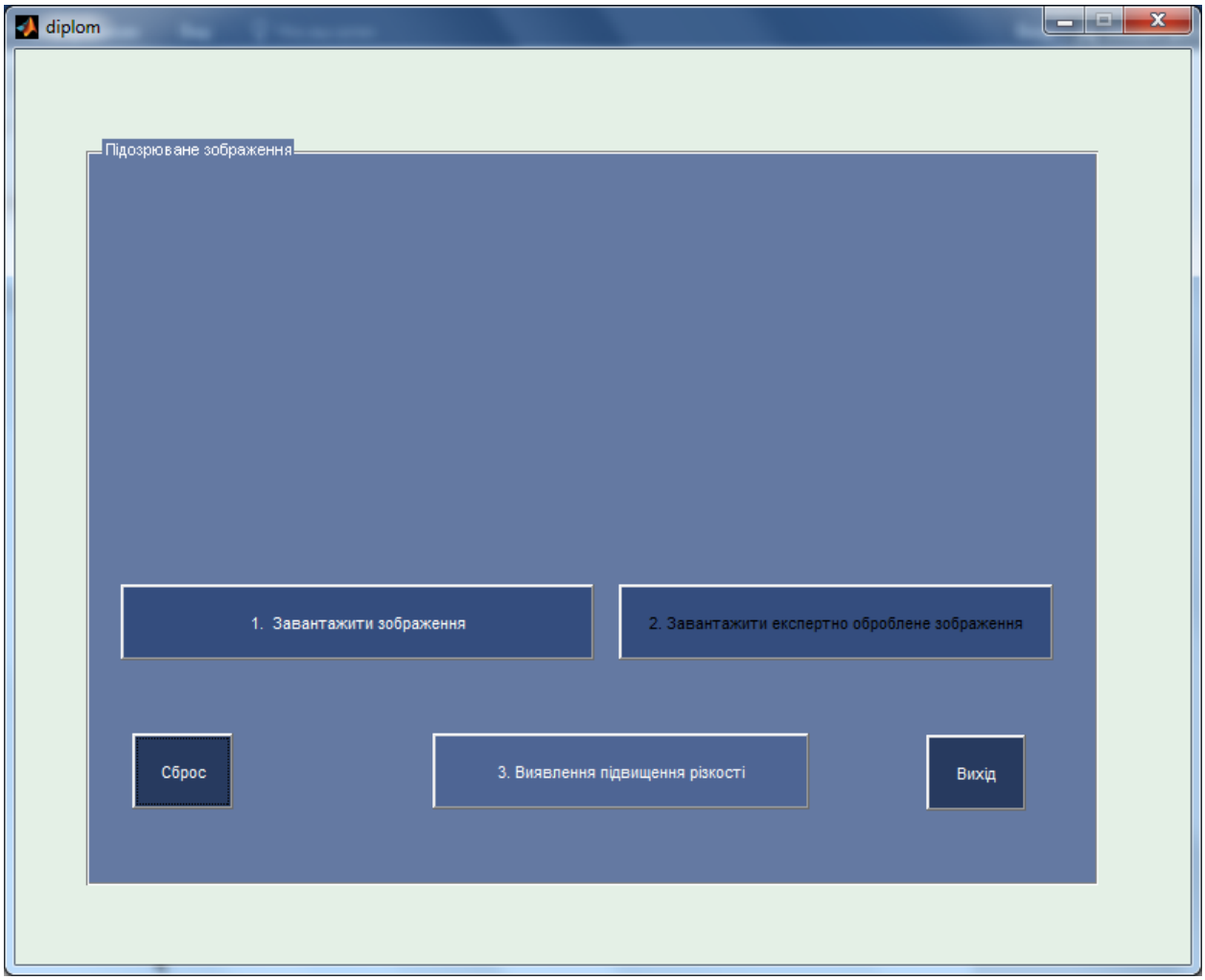


Рисунок 3.9 – Очищення від завантажених зображень

Програмний код дуже простий. Даний результат отримуємо шляхом застосування функції cla (рис.3.10).

```
function pushbutton4_Callback(hObject, eventdata, handles)
axes(handles.axes1);
cla
axes(handles.axes9);
cla
```

Рисунок 3.10 – Програмний код кнопки «Сброс»

Кнопка «Вихід» також є простою за своїм синтаксисом. Її програмний код представлено на рисунку 3.11.

```
function pushbutton5_Callback(hObject, eventdata, handles)
selection = questdlg(['Выход ' get(handles.figure1,'Name') '?'],...
                     ['Выход ' get(handles.figure1,'Name') '...'],...
                     'Да','Нет','Да');
if strcmp(selection,'Нет')
    return;
end
delete(handles.figure1)
```

Рисунок 3.11 – Програмний код кнопки «Вихід».

Один з важливих етапів, без якого використання даного програмного продукту не представляється можливим, це експертна обробка цифрового зображення. Експертна обробка виконується зовнішнім програмним забезпеченням, а саме графічним редактором GIMP. Даний графічний редактор обраний через можливість його вільного використання без необхідності придбання ліцензії, та, звичайно, через його багатофункціональність та можливості для обробки цифрових зображень.

Хоча і можна було реалізувати штучне підвищення різкості програмно засобами Matlab, однак вибір на користь зовнішнього програмного забезпечення було зроблено через те, що ймовірність використання власних засобів зловмисниками для підвищення різкості цифрового зображення в той час, коли значно легше та швидше можна скористатись графічним

редактором, дуже мала. До того ж, хоч обраний графічний редактор є вільним у використанні, але все ж свої реалізації фільтрів із зрозумілих причин власники не розголошують, тому власна реалізація могла б дати гірші результати й більшу кількість помилок першого й другого роду під час проведення експериментів. Тож, розглянемо етапи виконання процесу експертної обробки цифрового зображення.

Отже, після завантаження зображення у графічний редактор для застосування фільтру штучного підвищення різкості необхідно скористатись меню «Фільтри», обрати підпункт «Покращення», та натиснути на «Підвищити різкість (нерізка маска)» (рис.3.12).

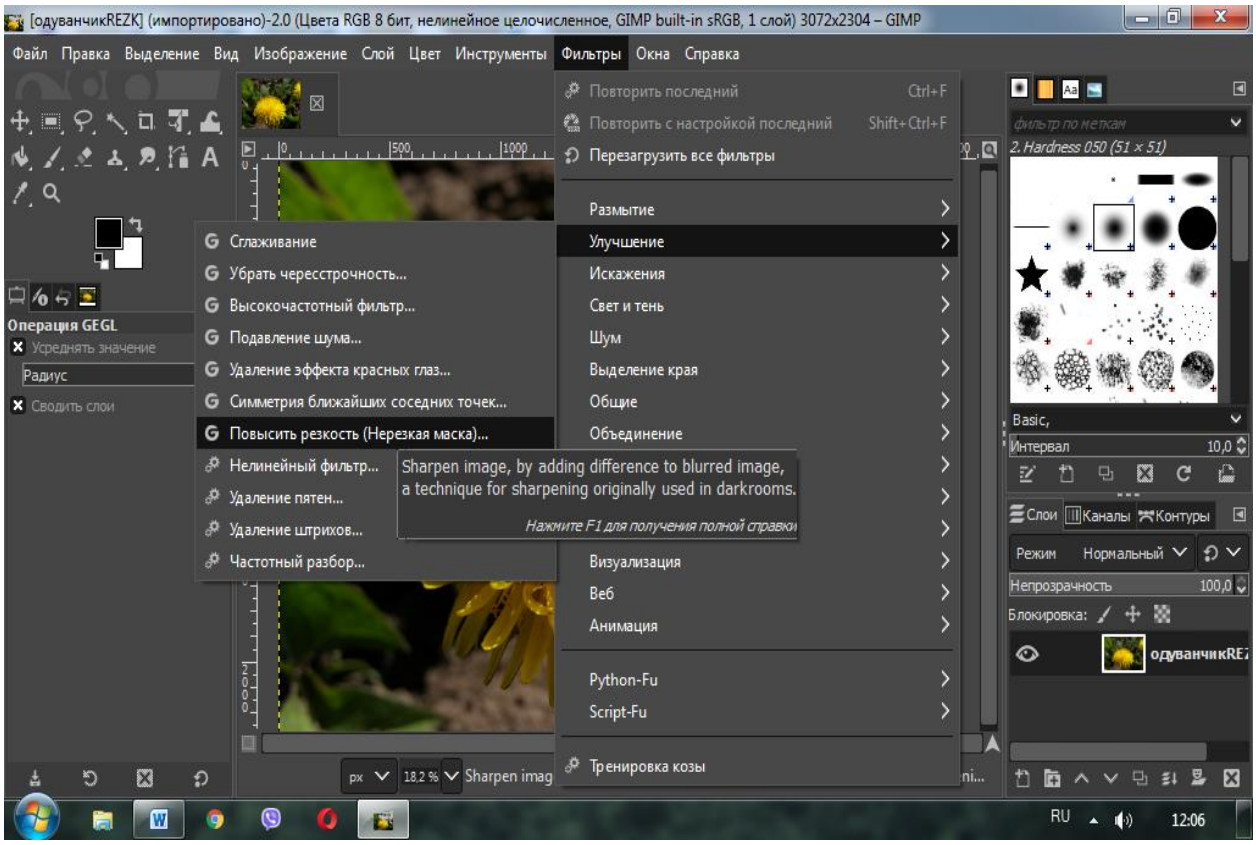


Рисунок 3.12 Пошук необхідного фільтру для експертної обробки зображення

Після вибору необхідного фільтру можемо бачити вікно настоюваних параметрів даного фільтру (рис.3.13). У даному вікні можна змінити параметри за замовчуванням під необхідний рівень підвищення різкості або для досягнення необхідного ефекту.

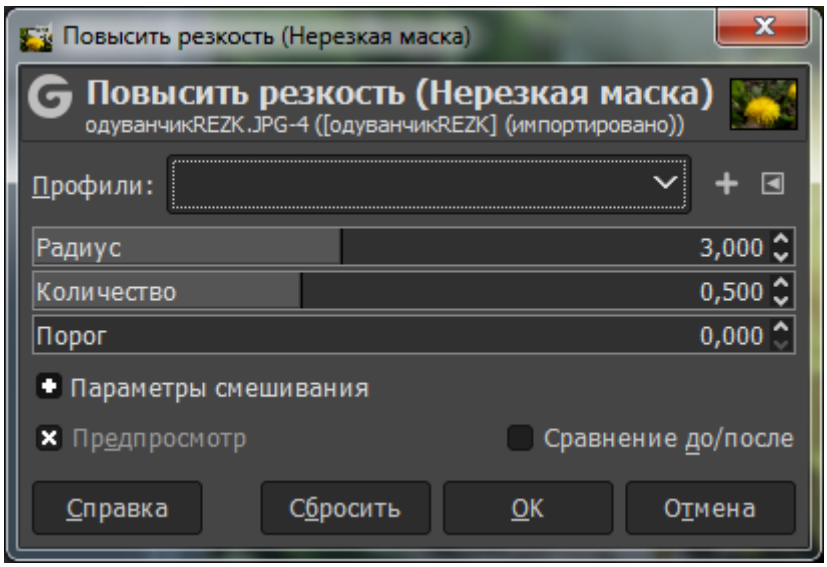


Рисунок 3.13 – Настроюванні параметри фільтру штучного підвищення різкості

Зміна даних параметрів призведе до гіпертрофії різкості на зображенні, що призведе до більшої чутливості методу виявлення до такої обробки. Тобто збільшення рівня різкості полегшить роботу запропонованого методу та зменшить помилки першого і другого роду. Проте в роботі радимо залишити параметри за замовчуванням.

Наступний етап – збереження обробленого зображення. Особливість обраного графічного редактора полягає в тому, що при стандартному збереженні цифрового зображення файл зберігається у форматі, з яким може працювати лише сам графічний редактор. Для бажаного збереження у відомих форматах, зокрема, форматі без втрат bmp, необхідно скористатись меню «Файл», обрати підпункт «Експортувати як…» та прописати ім’я та тип файлу з обранням місця збереження (рис.3.14, 3.15).

Після виконаних маніпуляцій зображення можна застосовувати для експертного виявлення штучного підвищення різкості засобами розробленого програмного застосунку.

Зважаючи на обставини відсутності кращих альтернатив та на доступність необхідного програмного забезпечення можна заключити, що реалізація методу задовольняє необхідним вимогам.

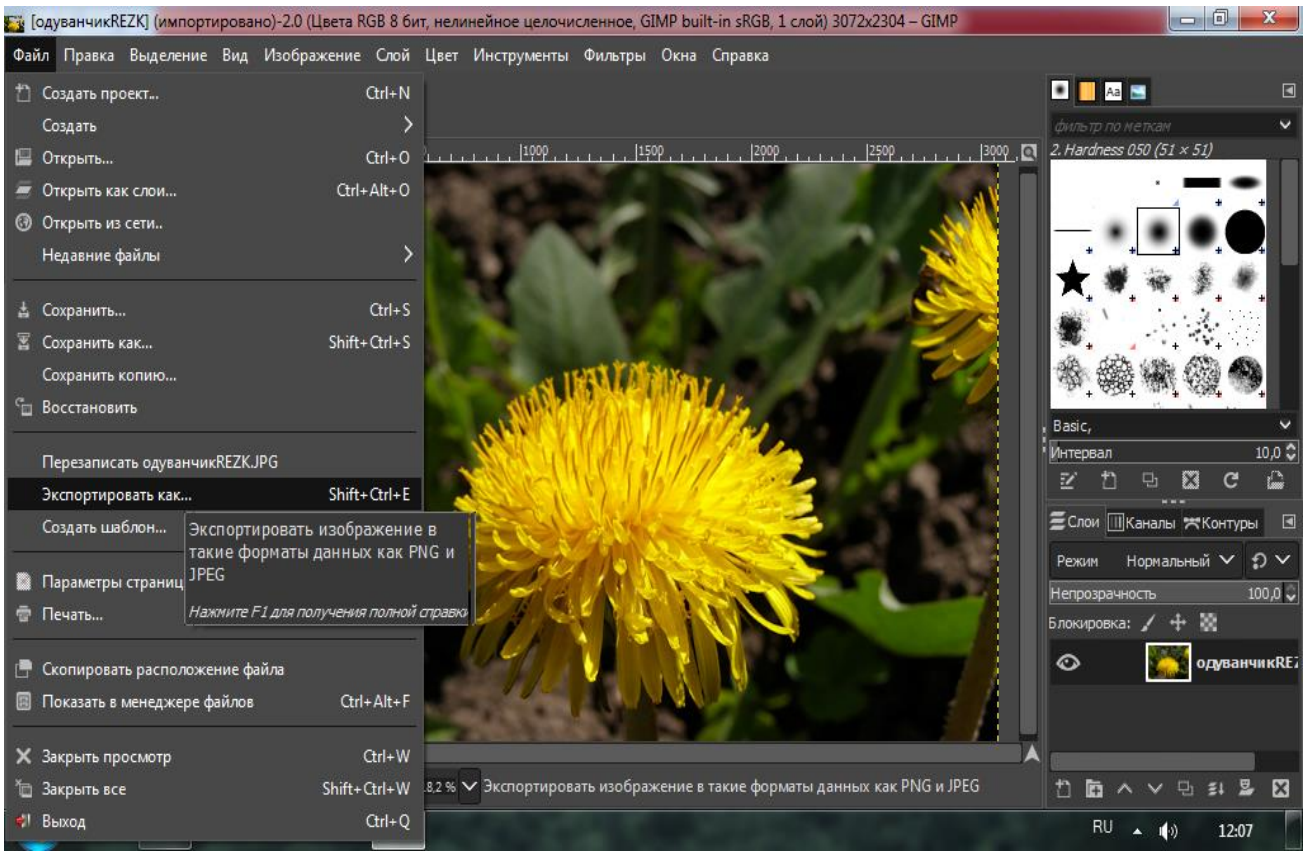


Рисунок 3.14 – Збереження файлу після його обробки

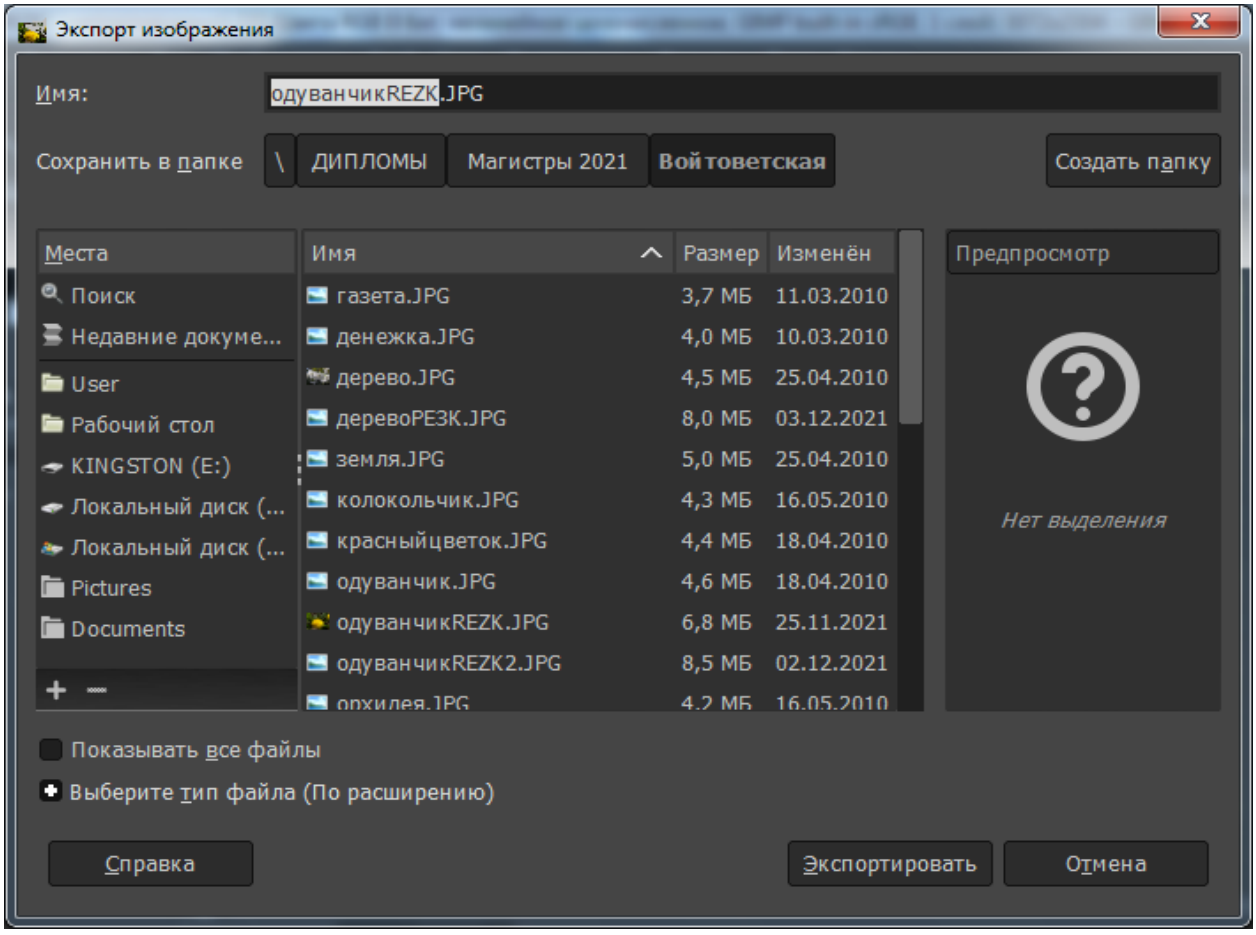


Рисунок 3.15 Налаштування параметрів збереження

У даному розділі виконано реалізацію модифікованого методу виявлення штучного підвищення різкості. Виконана реалізація є простою у використанні. Інтерфейс є інтуїтивно зрозумілим. Випробування його на фокус-групі дало змогу покращити функціонал та зробити його зручним для роботи експертів.

Даний програмний додаток можливо доопрацювати та внести до нього опції перевірки цифрових зображень на предмет наявності штучного підвищення різкості, якщо зображення після обробки було збережено у форматі з втратами. Також можна доповнити даний за стосунок іншими методами, направленими на пошук таких порушень цілісності, як розмиття, клонування, масштабування тощо.

4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів

Важливим завданням незалежно від форми власності і розміру організації є створення комфортних і безпечних умов праці для всіх фахівців згідно із законодавчими нормами конституції України (частина 4, стаття 43), закону «Про охорону праці» (розділ III, стаття 13), Кодексу законів про працю України, а також із нормативними вимогами державних стандартів, державних будівельних норм, санітарних норм і правил.

Трудова діяльність фахівця з кібербезпеки відбувається на робочому місці, обладнаному персональним комп'ютером.

Під час праці, пов'язаної із використанням комп'ютерів і інших периферійних пристроїв, виникають наступні небезпеки:

– енергетична небезпека внаслідок короткого замикання, її складові: електрична дуга, викид розплавленого металу, наслідок ураження електричним струмом – електричні опіки, електричні удари;

– пожежна небезпека;

– термічна небезпека, а саме вплив підвищених температур внаслідок нагрівання конструктивних елементів обчислювальної техніки; наслідки: нагрівання повітря в приміщенні, термічні опіки долонь і пальців;

– небезпека механічного травмування внаслідок падіння, дії рухомих частин обладнання, порізів гострими крайками конструктивних елементів;

– акустична небезпека: вплив високочастотних звукових коливань і вібрацій;

– небезпека електромагнітного випромінювання оптичного діапазону (інфрачервоного, ультрафіолетового, видимого світла і світла когерентної високої інтенсивності при використанні пристроїв, що використовують лазерне випромінювання);

– хімічна небезпека внаслідок контакту із хімічними речовинами, використовуваними при обслуговуванні устаткування.

Робочі місця розміщуються в приміщеннях офісного типу, зазвичай передбачають 2 – 4 місця в одному приміщенні. Кількість робочих місць визначають виходячи з умови, що на одне робоче місце слід відводити не менше ніж 6,0 $м^2$ площі і не менше ніж 20,0 $м^3$ об'єму приміщення. Існують певні вимоги щодо взаємного розташування робочих місць в приміщенні. Так, робочі місця слід розташовувати на відстані не менше ніж 1 м від стіни з віконними перерізами і на відстані не менше ніж 1,4 м від глухої стіни. Відстань між бічними поверхнями моніторів персональних комп'ютерів має бути не меншою за 1,2 м; відстань між тильною поверхнею одного монітора та екраном іншого повинна бути не менше ніж 2,5 м [31].

Окрім саме персональних комп'ютерів у приміщенні мають бути розташовані периферійні пристрої і меблі, необхідні для зручної організації робочого місця. Кожне приміщення обладнується системою електропостачання. Також воно обладнується засобами колективного захисту, які є елементами будівлі, а саме – системами природного освітлення, природної вентиляції, кондиціонування повітря, опалення.

Одним з важливих завдань охорони праці на робочому місці фахівця з кібербезпеки є збереження зорового здоров'я. Тому розглянемо засоби колективного захисту і вимоги щодо освітлення приміщень.

Приміщення з робочими місцями, обладнаними персональними комп'ютерами, повинні мати природне освітлення і бути облаштовані системою штучного освітлення.

Природне освітлення реалізується через вікна, орієнтовані бажано на північ або північний схід. Воно має забезпечувати коефіцієнт природної освітленості не нижче ніж 1,5 %.

Штучне освітлення слід реалізовувати системами загального освітлення, а в якості джерел світла рекомендується застосовувати люмінесцентні або світлодіодні лампи. Лампи слід встановлювати в

світильники, розташовані на стелі у вигляді суцільних або переривчастих ліній. Рекомендується застосування світильників двох наступних класів світлорозподілу: світильники прямого світла – клас П, і світильники переважно відбитого світла – клас В. Всі світильники мають бути обладнані розсіювачами і екрануючими пристроями. Застосування світильників без розсіювачів та екрануючих гратів заборонено. Також заборонено користуватись джерелами світла, не встановленими у світильники. Яскравість світильників загального освітлення із зоною кутів випромінювання 50° – 90° повинна складати не більше 200 кд/м^2, а захисний кут світильників повинен бути не менше 40°. Коефіцієнт запасу $К_з$ для систем штучного загального освітлення слід обирати у межах 1,4 – 1,5.

Системи штучного освітлення повинні створювати на поверхнях робочого місця нормовані значення освітленості, вказані в таблиці 4.1 [31].

Для забезпечення нормованих значень освітленості слід проводити генеральне прибирання і очищувати вікна та світильникИ не менше двох разів на рік. Також слід заміняти перегорілі джерела світла в світильниках.

В приміщеннях, в яких виконується робота переважно з екранами дисплеїв комп’ютерів, тривалістю не менш 50% робочого часу, слід створювати гігієнічні умови для зорової роботи. Для цього слід обмежувати нерівномірність розподілу яскравості в полі зору працівників, пульсацію освітленості в приміщенні, пряму і видбиту блискість, яскравість полисків на екрані і полисків великих поверхонь.

Задля більш рівномірного розподілу яскравості в полі зору працівників співвідношення яскравостей робочого екрана і близького оточення, а саме поверхні столу, документів не повинно перевищувати 5:1. Співвідношення яскравостей робочого екрана і більш далекого оточення, а саме периферійних пристроїв, стін, меблів не повинно перевищувати 10:1.

Для системи штучного освітлення пульсація освітленості не повинна перевищувати 5%. Люмінесцентні лампи, якщо їх використовують в

світильниках загального та місцевого освітлення, необхідно застосовувати разом із високочастотними пускорегулювальними апаратами.

Таблиця 4.1

Норми освітленості на робочих місцях із комп'ютерами

Характеристика роботи	Робоча поверхня	Освітленість
Робота переважно з екранами дисплеїв ПК (50 % та більше робочого часу)	Екран	Не вище 200 лк
	Клавіатура	Не нижче 400 лк
	Стіл	Не нижче 400 лк
Робота переважно з документами (50 % та більше робочого часу)	Екран	Не вище 200 лк
	Клавіатура	Не нижче 400 лк
	Стіл	Не нижче 500 лк
Основні проходи	Підлога	Не нижче 100 лк

Пряма блискість від джерел природнього та штучного освітлення повинна бути обмежена. Тому яскравість вікон і джерел світла, що опиняються у полі зору працівника, не повинна перевищувати 200 кд/м^2.

З метою захисту від прямої блискості в полі зору працівника необхідно знижувати яскравість видимої частини джерел світла. Для цього застосовують розсіювачі і відбивачі світла на арматурі. Крим того, слід контролювати розміщення робочих місць відносно джерел світла.

З метою обмеження відбитої блискості на робочих поверхнях в полі зору працівника, наприклад, на екрані, клавіатурі, поверхні столу, слід контролювати яскравість цих поверхонь. Наприклад, яскравість стелі при розміщенні на неї світильників класу В (відбитого світла) не повинна перевищувати 200 кд/м^2. Полискі на екрані повинні мати яскравість не більше 80 кд/м^2.

Важливе значення має колірна гармонія робочих поверхонь, поверхонь стін і меблів в приміщенні, оскільки палітра кольорів є інструментом для

створення психологічного комфорту і остаточно – підвищення продуктивності праці. Найбільш сприятливими для органів зору є неяскраві світлі тони: відтінки зеленого, синього, блакитного, світло-сірий, бежевий. Яскраві елементи декору, поєднання контрастних кольорів (наприклад, жовтого і синього, червоний і зеленого, чорного і білого) відволікають, роздратовують органи зору, викликають втому.

Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях

Техногенна небезпека – стан, внутрішньо притаманний технічній системі або виробничому об'єкту, що реалізується у вигляді негативних впливів на людину і навколишнє середовище при виникненні надзвичайної ситуації, або у вигляді прямої чи опосередкованої шкоди для людини і навколишнього середовища в процесі нормальної експлуатації цих об'єктів.

Надзвичайні ситуації техногенного характеру за характеристиками явищ, що визначають особливості дії факторів ураження, поділяють на аварії, які супроводжуються викидами шкідливих речовин, пожежі, вибухи, аварії в інженерних мережах і системах життєзабезпечення, руйнування будівель і споруд, аварії на транспортних засобах.

За статистичними даними, найбільш імовірною техногенною небезпекою в приміщеннях, в яких розміщені робочі місця фахівців з кібербезпеки, є пожежі.

Основні причини виникнення пожеж:

– експлуатація несправної або морально застарілої обчислювальної техніки;

– пошкодження або відсутність систем захисного заземлення обчислювальної техніки;

– експлуатація обчислювальної техніки із пошкодженою ізоляцією проводів і мереж зв'язку;

– підключення обчислювальної техніки до пошкоджених розеток;

– обгортання світильників місцевого освітлення горючими матеріалами, наприклад, папером або тканиною;

– нагромадження паперових документів на корпуси обчислювальної техніки;

– підключення до мережевих фільтрів, блоків безперебійного живлення і спеціалізованих розеток електронагрівальних пристроїв, побутової техніки та іншого обладнання, що не належить до обчислювальної технікі.

З метою забезпечення вимог електробезпеки і пожежовибухобезпеки всі персональні комп'ютери, периферійні пристрої, оргтехніка, кабелі мережі Інтернет повинні мати виконання та ступень захисту відповідно вимог ПУЕ. Підключати вказану техніку слід із використанням апаратури захисту від перевантаження, стрибків напруги, короткого замикання та інших аварійних режимів. До засобів колективного захисту належать пристрої захисного заземлення, захисного занулення, захисного відключення.

В кожному приміщенні мають бути розміщені засоби первинного пожежогасіння, а саме порошкові або вуглекислотні вогнегасники. Норма розміщення вогнегасників – один вогнегасник на кожні 50 м^2 площі приміщення, але не менш ніж 1 вогнегасник на приміщення.

Вогнегасники слід розміщати таким чином, щоб вони були захищені від прямих сонячних променів, механічних впливів і інших несприятливих факторів (вібрація або підвищена вологість). Вогнегасники слід розміщувати в помітних і легкодосяжних місцях. Кожен співробітник обов'язково має бути ознайомлений з правилами експлуатації вогнегасників. На кожен вогнегасник необхідно мати сертифікат якості.

Проектування системи освітлення

За вимогами охорони праці, основним засобом колективного захисту, призначеним для оптимізації умов зорової і розумової праці в приміщеннях із обчислювальною технікою є система загального штучного освітлення.

Вихідні дані для її проектування:

– фактична освітленість на робочих місцях (на поверхні столу): $E_ф$ =

250 лк;

– розміри приміщення: довжина A = 18 м; ширина B = 15 м;

– розрахункова висота підвісу світильника: H = 2,8 м;

– найменший розмір об’єкта розрізнення: 0,35 мм;

– контраст об’єкта розрізнення з фоном великий, фон світлий;

– система освітлення: загальна, виконується світильниками ЛВПЗЗ з люмінесцентними лампами;

– концентрація пилу в повітрі: 1,0 мг/м^3;

– коефіцієнти відображення: 0,5 – 0,3 – 0,1.

За найменшим розміром об’єкта розрізнення визначаємо розряд зорової роботи: III розряд, роботи підвищеної точності [32]. Для III розряду зорової роботи норма освітленості на робочому місці становить: $E_н$ = 400 лк. Таким чином, фактична освітленість на робочих місцях недостатня: $E_ф$ = 250 лк, що менше нормативної освітленості $E_н$ = 400 лк. Тому існує необхідність модернізувати існуючу систему освітлення. Виконуємо її розрахунок [33].

Площа приміщення:

$$S = AB = 18 \cdot 15 = 270 \text{ м}^2$$

Індекс приміщення:

$$i = \frac{S}{(A+B)\cdot H} = \frac{270}{(18+15)\cdot 2,8} = 2,92$$

Еквівалентна площа:

$$S_e = \frac{S \cdot K \cdot z}{\eta} = \frac{270 \cdot 1,9 \cdot 1,05}{0,33} = 1632 \text{ м}^2.$$

Оптимальна кількість світильників:

$$N_o = \frac{S}{L_o^{\,2}} = \frac{270}{3^2} = 30 \text{ шт.}$$

Приймаємо N_o = 30 шт.

Потрібний світовий потік світильників:

$$\Phi_c = \frac{S_e \cdot E_н}{N_o} = \frac{1632 \cdot 400}{30} = 21760 \text{ лм.}$$

Освітленість E_1, яка створюється одним світильником:

$$E_1 = \frac{n \cdot Ф}{S_e} = \frac{4 \cdot 21760}{1632} = 54 \text{ лк.}$$

Кількість світильників:

$$N_n = \frac{E_н}{E_1} = \frac{400}{54} = 7,4 \text{ шт.}$$

Приймаємо остаточну кількість світильників для монтажу N = 8 шт.

За розрахунком в приміщенні необхідно встановити загальну систему штучного освітлення з 8 світильників типу ЛВПЗ3, кожен із 4 із люмінесцентними лампами, які рекомендується рівномірно розташувати на стелі в два ряди по 4 світильники.

ВИСНОВКИ

В роботі проведено аналіз джерел з виявлення порушень цілісності цифрового зображення. В результаті аналізу встановлено, що проблема виявлення підробок цифрових зображень не є вирішеною до кінця. Зокрема, виявленню такого порушення цілісності як штучне підвищення різкості цифрового зображення приділено мало уваги.

Для цифрового зображення в якості параметрів для аналізу на предмет наявності в ньому штучного підвищення різкості обрано матриці яскравостей пікселів.

Проведено обчислювальний експеримент з використанням 600 цифрових зображень. Усі зображення було оброблено фільтром фоторедактору GIMP «Unsharp Mask» та збережено у форматі без втрат.

Було встановлено порогове значення для відділення оброблених цифрових зображень від необроблених.

На основі проведених експериментів та отриманих результатів було модифіковано метод виявлення штучного підвищення різкості цифрового зображення. Помилки першого роду склали 4%, помилки другого роду 7%.

Модифікований метод реалізовано у програмному середовищі Matlab. Програмний продукт є прости у використанні, має інтуїтивно зрозумілий інтерфейс.

ПЕРЕЛІК ПОСИЛАНЬ

1. Зоріло В.В., Берія Д.Ю., Войтовецька М.Є., Козаченко Н.Г., Лебедєва О.Ю. Виявлення порушень цілісності цифрових зображень в контексті цифрової криміналістики. *Інформатика та математичні методи в моделюванні*.. 2022. №1-2. С. 56-60.

2. Зорило В.В., Колісніченко Ю.С. Вплив розмиття різного радіусу на властивості матриці цифрового зображення. *Матеріали міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології»*. 2013р. Одеса. С.7-9.

3. Хорошко В.А.,Чекатков А.А. Методы и средства защиты информации. Научное издание. К.: ЮНИОР, 2003. 505с.

4. Ленков С.В., Хорошко В.А. Методы и средства защиты информации: в 2 т. К.: Арий, 2008. 213 с. Т.2: Информационная безопасность. 2008. 344 с.

5. Нариманова Е.В. Проверка целостности цифрового сигнала. Монографія. Донецк. Изд. Цифровая типография, 2011. 180 с.

6. Фетняев И.Ю. Признаки монтажа и других изменений в цифровых фонограммах и фотографіях. *Сборник трудов XVIII международной научной конференции "Информатизация и информационная безопасность правоохранительных органов".* Москва, 2009. С. 229-235.

7. Грибунин В.Г. Цифровая стеганография. Монография. М.: СОЛОН-Пресс, 2002. 272с.

8. Fridrich, J. Methods for Tamper Detection in Digital Images. ACMMM&SEC 1999: Proceedings of the Multimedia and Security Workshop 1999, 30 October 1999. Orlando, Florida, USA, 1999. P.19-23.

9. Fridrich, J. Protection of digital images using self-embedding. *Proceedings of Symposium on Content Security and Data Hiding in Digital Media*. May 1999. Newark, New Jersey, USA, 1999. P. 92-96.

10. Fridrich J. Images with self-correcting capabilities. ICIP 1999.

Proceedings of IEEE International Conference on Image Processing. 25-28 October 1999. Kobe, Japan, 1999. Vol.3. P. 792-796.

11. Yeung M.M. An Invisible Watermarking Technique for Image Verification. ICIP 1997. *Proceedings of IEEE International Conference on Image Processing.* 26-29 October 1997. Santa Barbara, California, USA. 1997. Vol.2. P. 680-683.

12. Wolfgang, R. B. A Watermark for Digital Images. ICIP 1996. *Proceedings of IEEE International Conference on Image Processing.* 16-19 September1996. Lausanne, Switzerland, 1996. Vol.3. P. 219-222.

13. Dybala B. Detecting filtered cloning in digital images. *In ACM Multimedia and Security Workshop*. 2007. P. 43-50.

14. Langille A. An efficient match-based duplication detection algorithm. *In Canadian Conference on Computer and Robot Vision.* 2006. P.64.

15. Luo W. Robust detection of region duplication forgery in digital images. *In International Conference on Pattern Recognition.* 2006. P.746-749.

16. Pan X. Region duplication detection using image feature matching. *IEEE Transactions on Information Forensics and Security.* 2010. Vol.5(4). P.857-867.

17. Wang J. Detection of image region duplication forgery using model with circle block. *In International Conference on Multimedia Information Networking and Security.* 2009. P. 25-29.

18. Jing L. Image Copy-Move Forgery Detecting Based on Local Invariant Feature. *Journal of Multimedia*. Feb, 2012. Vol 7, No 1. P.90-97.

19. Shivakumar B.L. Detection of Region Duplication Forgery in Digital Images Using SURF. *IJCSI International Journal of Computer Science Issues.* July, 2011. Vol.8, Issue 4, No 1. P.199-205.

20. Bay H. SURF: Speeded Up Robust Features. *ECCV.* 2006. Vol.1. P.404-417.

21. Lowe D.G. Distinctive image features from scale-invariant keypoints URL: http://www.cs.ubc.ca/~lowe/papers/ijcv04.pdf.

22. Popescu A.C. Statistical tools for digital forensics. *The 6th International Workshop on Information Hiding.* 23-25 May, 2004. Toronto, Canada, 2004. P. 128-147.

23. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монографія. К.: ГУИКТ, 2009. 251 с.

24. Зорило В.В. Методы повышения эффективности выявления нарушения целостности цифрового изображения. *Інформаційна безпека.* 2012. №1(7). С.8

25. Кобозева А.А., Рыбальский О.В., Трифонова Е.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала. *Вісник Східноукраїнського національного університету ім. В. Даля.* 2008. №8(126), Ч.1. С. 62-72.

26. Кобозева А.А. Математические основы общего подхода к обнаружению фальсификации цифрового сигнала. *Материалы Международной научно-технической конференции «Искусственный интеллект. Интеллектуальные системы ИИ-2008».* 2008. Т.2. С.32-35.

27. Кобозева А.А. Использование теории возмущений для обнаружения фальсификации цифрового изображения. Проблеми інформатизації та управління. *Матеріали міжнародної науково-технічної конференції «Комп'ютерні системи та мережні технології». Збірник наукових праць.* 2008. №1(23). С.16-22.

28. Кобозева А.А. Использование теории возмущений для установления подлинности цифрового изображения. *Труды девятой международной научно-практической конференции «Современные информационные и электронные технологии СИЭТ-2008».* 2008. Одесса, С.69.

29. Zorilo V.V., Pyvovar O.V., Safronov P.S. Histogram analysis for detection of sharpened digital images. *Інформатика та математичні методи в моделюванні.* Том 9, № 3. 2019р. С.279-283.

30. NRCS Photo Gallery. United States Department of Agriculture.

Washington, USA. URL: http://photogallery.nrcs.usda.gov

31. ДСанПіН 3.3.2.007–98. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.

32. ДБН В.2.5-28-2006 Природне і штучне освітлення

33. Методичні вказівки до лабораторної роботи «Дослідження штучного освітлення у виробничих приміщеннях» для студентів усіх спеціальностей / Упоряд. С.С. Головатюк. Одеса: ОНПУ, 2004. 30 с.