Міністерство освіти і науки України

Державний університет «Одеська політехніка»

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Войтовецька Марія Євгеніївна,

студентка 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 з втратами

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

Войтовецькій Марії Євгеніївни

1.Тема роботи: *Модифікація метода виявлення підвищення різкості для цифрового зображення (комплексна). Модифікація метода виявлення підвищення різкості для цифрового зображення у форматі з втратами*.
керівник роботи *Зоріло Вікторія Вікторівна, к. т. н.,*
затверджені наказом ректора університету від „25” жовтня 2021 р. №372-в.
2.Зміст роботи*: аналіз існуючих методів виявлення фальсифікацій 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 _____ *Войтовецька М.Є.*

Керівник роботи _____ *Зоріло В.В.*

ЗАВДАННЯ

на розробку розділу «Охорона праці»

Войтовецькій Марії Євгеніївні, 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 з втратами.*

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 загального штучного 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 з втратами» на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 – Кібербезпека містить 18 рисунків, 7 таблиць, 17 літературних джерел за переліком посилань. Робота виконана на 48 сторінках загального тексту і 36 сторінках основного тексту.

Метою цієї роботи стало підвищення ефективності виявлення обробки цифрового зображення шляхом модифікації методу виявлення підвищення різкості.

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 8%, другого роду – 10%.

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 loss format"for the second (master's) level of higher education in the specialty 125 – Cybersecurity contains 18 figures, 7 tables, 17 references at the list of references. The work is performed on 48 pages of general text and 36 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 8%, the second kind - 10%.

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

ЗМІСТ

ВСТУП 8
1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ 10
1.1 Проблема фальсифікації цифрових зображень 10
1.2 Методи виявлення підробок цифрових зображень в цифровій криміналістиці 13
1.3. Аналіз сучасних методів виявлення зашумлення зображень 15
2 МОДИФІКАЦІЯ МЕТОДУ ВИЯВЛЕННЯ ШТУЧНОГО ПІДВИЩЕННЯ РІЗКОСТІ 18
2.1 Основні положення методу виявлення штучного підвищення різкості 18
2.2 Дослідження ефекту «піку чорного» для зображень у форматі з втратами 20
2.3 Модифікований метод 27
3 РЕАЛІЗАЦІЯ МОДИФІКОВАНОГО МЕТОДУ 28
4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 37
ВИСНОВКИ 46
ПЕРЕЛІК ПОСИЛАНЬ 47

ВСТУП

У наш час цифрові зображення відіграють надзвичайно важливу роль у багатьох сферах застосування. Але в той же час збільшились і методи редагування зображень. За часів до того, як програмне забезпечення для обробки зображень стало настільки широко доступним, внесення змін до зображення вимагало значних зусиль та досвіду. Зараз дуже просто, і тому спокусливо, вносити зміни до цифрових зображень, що створює серйозну загрозу їх безпеці.

Експертиза цифрових зображень стає все більш важливою, оскільки цифрові зображення несуть важливу інформацію завдяки їх використанню в різних сферах: юридичній, медичній, журналістиці, цифровій криміналістиці, наукових публікаціях тощо.

Метою цієї роботи стало підвищення ефективності виявлення обробки цифрового зображення шляхом модифікації методу виявлення підвищення різкості. Для цього були поставлені наступні задачі:

- проаналізувати доступні джерела з виявлення порушень цілісності цифрових зображень;
- визначити параметри цифрового зображення для аналізу;
- провести обчислювальний експеримент з використанням зображень, оброблених фільтром штучного підвищення різкості зі збереженням зображень у форматі з втратами;
- розробити і реалізувати алгоритм виявлення обробки зображення фільтром штучного підвищення різкості;
- розробити призначений для користувача інтерфейс програмного продукту.

Об’єктом дослідження є процес виявлення фальсифікації цифрового зображення.

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

Практичне значення одержаних результатів. Результатом роботи є модифікований метод виявлення штучного підвищення різкості цифрового зображення у форматі з втратами 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 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ

1.1 Проблема фальсифікації цифрових зображень

У наш сучасний вік цифрові зображення відіграють надзвичайно важливу роль у багатьох сферах застосування. Але в той же час збільшились і методи редагування зображень. За часів до того, як програмне забезпечення для обробки зображень стало настільки широко доступним, внесення змін до зображення вимагало значних зусиль та досвіду. Зараз дуже просто, і тому спокусливо, вносити зміни до цифрових зображень, що створює серйозну загрозу їх безпеці.

Автентифікація цифрових зображень стає все більш важливою, оскільки цифрові зображення несуть важливу інформацію завдяки їх використанню в різних сферах: юридичній, медичній, журналістиці, цифровій криміналістиці, наукових публікаціях тощо.

На сьогоднішньому рівні розвитку цифрові технології можуть імітувати майже все – музику, голос, зображення, рухомі об'єкти. Будь-які звуки генеруються в сучасних аудіоредакторах.

Створити графічне зображення, яке буде схоже на звичайну фотографію, можна в графічному редакторі. У програмах 3D-моделювання створюються рухливі моделі, які неможливо відрізнити від об'єктів реальної відеозйомки. Всім цим дуже легко ввести в оману людей.

Цифрові зображення часто використовуються в суді в якості речового доказу або демонстративного матеріалу [2]. Тим не менше, ніколи не було так легко зробити так, щоб фотографії спотворювали правду, ніж зараз. Важливо визначити, чи є інформація, надана слідству, правдивою та чи не спотворена вона.

Демонстративні докази можуть бути потужним інструментом, який допомагає присяжним зрозуміти важку концепцію, підкріпити їхні переконання, або навіть переконати їх повірити у щось. Правила допуску

демонстративних доказів є менш суворими, ніж для речових доказів, що створює ще більший потенціал для допущення фальсифікованих цифрових зображень.

Ще однією галуззю, де фальсифікація зображень є важливою проблемою – це наука. Хороша наука вимагає надійних даних. Отже, все більше наукових журналів вживають заходів для вирішення зростаючої проблеми фальсифікації і маніпулювання зображеннями в статтях, поданих до них для публікації.

У вересні 2018 року в журналі Scientific Reports було опубліковано суперечливу статтю [2], в якій стверджувалося, що гомеопатичний препарат з рослини отруйного плюща може полегшити біль у щурів. Незважаючи на те, що спочатку шум відбувся через запеклу дискусію щодо ефективності гомеопатії, він посилився, коли виявилося, що стаття має фальсифіковане зображення [3].

Ще один приклад стався, коли дослідники, пов'язані з Міжнародним агентством Всесвітньої організації охорони здоров'я з дослідження раку (IARC), робили маніпулювання зображеннями в багатьох наукових роботах, які вони публікували протягом багатьох років. У період між 2005 і 2014 роками Массімо Томмазіно, керівник групи інфекцій та біології раку в IARC у Ліоні, Франція, та його колишній колега Узма Хасан опублікували безліч статей із підробленими зображеннями [4].

Відредаговані фотографії в дослідженнях, як правило, можуть бути будь-якими – від мікроскопічних оглядів клітин до навіть графічного подання даних. Маніпуляції з зображеннями в дослідницькій роботі можуть мати серйозні наслідки.

На нараді з плагіату в Лондоні в 2009 році, Вірджинія Барбур, головний редактор журналу PLoS Medicine, повідомила, що проблема маніпуляції зображеннями «підкралася» до редакторів журналів з моменту появи редагуючого програмного забезпечення, такого як Photoshop або Gimp [5].

У 2018 році була запущена база даних із 18 000 відкликаних наукових робіт, що робить її найбільшою у своєму роді. З них 317 робіт було відкликано через фальсифікації зображень – що становить приблизно 1,7 відсотка від загальної кількості робіт [6].

Часто потрібно більше, ніж добре навчене око, щоб виявити такі маніпуляції. Тут дуже доречні інструменти цифрової криміналістики. Програмне забезпечення використовується для виявлення навмисних змін зображень у наукових роботах. Навчання людей користуванню такими ресурсами також може зайняти час, але, як показують ці тривожні висновки, це є важливим для гарантування достовірності та наукової обґрунтованості.

Протидія поведінці дослідників існувала завжди, але ця тема викликає дедалі більшу стурбованість з огляду на гучні скандали, кризу відтворюваності та епідемію відкликаних статей, більшість з яких спричинені неправомірною поведінкою. Продовження присутності скомпрометованих статей у літературі може мати згубний вплив на прогрес науки, вводячи дослідників в оману у своїх галузях.

Крім того, поширеність фальсифікованих фотографій викликає важливе запитання: чи можуть люди виявляти підробки фотографій. У дослідженні [7] було проведено два експерименти, де дослідники попросили людей виявити та локалізувати маніпуляції на зображеннях реальних сцен. Учасники експерименту продемонстрували обмежену здатність виявляти оригінальні та підроблені зображення.

Крім того, в обох експериментах, навіть коли суб'єкти правильно виявляли фальсифіковані зображення, вони часто не могли знайти маніпуляцію. Із зазначеного можна зробити висновки, що люди погано здатні визначити, чи зображення є оригінальним чи до нього вносились зміни. Усе це вказує на необхідність створення автоматизованих систем виявлення порушень цілісності цифрових сигналів загалом, та цифрових зображень зокрема. Розглянемо деякі сучасні методи, що дозволяють уникнути необхідності експертної оцінки автентичності зображень.

1.2 Методи виявлення підробок цифрових зображень в цифровій криміналістиці

Оскільки люди загалом вірять у те, що бачать, існує важлива і нагальна потреба у розробці методів, які здатні перевірити справжність та надійність зображень. Нажаль, немає простого рішення, щоб запобігти обману людей за допомогою підроблених фотографій у повсякденному житті або на кримінальній арені. Щоб впоратися з проблемою фальсифікації зображень, виникла сфера криміналістики цифрових зображень як основна галузь знань, зосереджена на перевірці справжності та цілісності цифрових зображень, яка забезпечила певну довіру до них. Важливість і актуальність криміналістики цифрових зображень залучила різних дослідників до створення різних методів виявлення фальсифікації зображень.

Підробка зображення – це створення фальшивого зображення шляхом зміни вмісту оригінального зображення та створення його як оригінальної фотографії для незаконних цілей.

Криміналістика зображень прагне виявити докази підробок. В ній розглядається питання автентифікації зображень або їх походження та надаються достовірні відповіді щодо походження та справжності цифрових зображень.

Криміналістика зображень використовує цифрові технології для визначення справжності зображення і базується на передумові, що цифрові маніпуляції змінюють значення пікселів, з яких складається зображення. Простіше кажучи, акт маніпулювання фотографією залишає за собою слід, навіть якщо вона неявна і не видна неозброєним оком. З огляду на те, що різні типи маніпуляцій – наприклад, клонування, ретуш, зрощення – впливають на основні пікселі унікальним і систематичним способом, експерти-криміналісти можуть розробити комп’ютерні методи для виявлення підробок зображень.

Зображення, відредаговані за допомогою програмних засобів, проходять кілька етапів обробки та настільки фотореалістичні, що підробка

зображення найчастіше не може бути виявлена людським зором. Як наслідок, фальсифіковані зображення з’являються все частіше, що призводить до зменшення довіри до візуального вмісту. Отже, достовірність зображення не сприймається як належне. З розвитком інструментів для підробки було впроваджено технології перевірки оригінальності інформації про зображення.

Семантична інформація зображення змінюється шляхом додавання або вилучення інформації із зображення. Для того, щоб досягти фальсифікування зображення, зловмисники використовують численні способи. Загалом існують різні типи підробки зображень. Класифікація видів підробки зображень є нудним завданням; це пов’язано з тим, що типи підробки групуються на основі процесу, пов’язаного зі створенням фальшивого зображення. Але в сучасному технічному світі в цифрову фотографію вносяться нові інновації, які з кожним днем підштовхують до розробки нових методів фальсифікування.

Методи виявлення цифрової підробки зображень поділяються на два підходи: активний та пасивний [8]. При активному підході цифрове зображення вимагає попередньої обробки зображення, наприклад, вбудовування водяних знаків або формування електронного підпису. Однак для цього типу технологій потрібно спеціальне програмне або апаратне забезпечення, щоб вставити або витягти інформацію.

На відміну від методів, що базуються на водяних знаках та підписах, пасивні методи не потребують цифрового підпису чи вбудовування будь-якого водяного знаку.

Криміналістика зображень, як правило, є великим випробуванням у техніці обробки зображень. Не існує конкретного методу, який може виявляти всі ці випадки, але є багато методів, кожен з яких може виявити певну підробку по-своєму.

Виявлення підробки є альтернативою активній автентифікації, яка не вимагає наявності активної інформації для цілей автентифікації. Ці методи

виявляють підробку, аналізуючи статистику зображення за відсутності водяних знаків, а також оригінальне зображення для порівняння. Локалізація фальсифікацій базується виключно на статистиці характеристик цифрових зображення.

Виявлення модифікації цифрового зображення за допомогою шуму – дуже важлива задача, оскільки зміст зображення буде змінено. Таким чином, зображення не може відігравати свою важливу роль як доказ. Тому автентифікація цифрових зображень дуже важлива і робить судово-медичну науку вкрай необхідною.

1.3. Аналіз сучасних методів виявлення зашумлення зображень

Основний підхід, який використовується в переважній більшості алгоритмів, полягає в аналізі ковзного вікна [9]. Під ковзним вікном розуміється деяка локальна область зображення, яка послідовно проходить всі пікселі. З порівняння характеристик центрального пікселя вікна з іншими пікселями вікна робиться висновок про його пошкодження.

Відмінність методів детектування пошкоджених пікселів один від одного полягає у виборі розмірів ковзного вікна і алгоритму прийняття рішення про пошкодження пікселя [10-12]. Однак ефективність пошуку пошкоджених пікселів істотно залежить від налаштувань. Наприклад, алгоритм SD-ROM, що лежить в основі великої кількості інших алгоритмів, містить чотири параметри, які вибираються користувачем. Варіювання даних параметрів може змінювати ефективність пошуку пошкоджених пікселів від 62% до 96%. При цьому залишається високим відсоток помилкових спрацьовувань.

Поліпшення результатів вдається домогтися з використанням алгоритмів, які аналізують не тільки невелику локальну область, а й все зображення в цілому. В якості таких можна відзначити алгоритми на основі асоціативних правил, методах підтримки прийняття рішень, а також засновані на методах сегментації зображень. У всіх перерахованих

алгоритмах один або два настроюваних параметра і досить висока ефективність виявлення пошкоджених пікселів. При цьому вдається істотно знизити відсоток помилкових спрацьовувань.

В результаті огляду джерел, було виявлено, що існуючі методи все ще не достатньо ефективно вирішують проблему фальсифікації ЦЗ, зокрема шляхом накладання шуму, тому дана проблема актуальна та вимагає пошуку її вирішення.

Одним з програмних інструментів для зашумлення цифрового зображення є штучне підвищення різкості цифрового зображення. Даний фільтр є протилежним за дією фільтру розмиття за Гаусом й іншим фільтрам, що мають своєю метою розмиття контурів зображення.

Виявлення його за допомогою швидкості росту сингулярних чисел не досліджене й ускладнене тим, що сучасні зображення з високою глибиною різкості зображуваного простору часто мають настільки високу швидкість росту відповідних сингулярних чисел, що і у тих зображеннях, які оброблено фільтром. Має сенс провести додаткові дослідження з цієї теми й зайнятись пошуком іншого інструменту для виявлення цього виду обробки цифрового зображення.

У роботі [13] було зафіксовано ефект «піку чорного» у всіх трьох колірних компонентах матриці цифрового зображення. Експеримент було проведено за допомогою графічного редактора GIMP, де цифрові зображення було оброблено фільтром «Unsharp mask» із параметрами за замовчуванням. Після застосування даного фільтру було помічено одну особливість, яка дала змогу виявити застосування обробки. Варто зауважити, що у проведених і описаних експериментах зображення після обробки було збережено у форматі без втрат.

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

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 даному розділі проведено аналіз джерел, доступних у відкритому друці, за темою виявлення порушень цілісності ЦЗ. Зашумлення цифрових зображень часто застосовують зловмисники задля приховання слідів зміни сцен цифрових зображень, або з метою скоїти стеганографічну атаку на цифрове зображення.

Також з аналізу джерел стало відомо, що виявлення зашумлення в цілому й фільтрації, що призводить до підвищення різкості цифрового зображення зокрема, приділено недостатньо уваги. Метод виявлення штучного підвищення різкості, про який відомо з відкритого друку, пройшов випробовування лице при збереженні цифрових зображень після фальсифікації у форматі без втрат. Утім, на даний момент більшість цифрових зображень все ж зберігається у форматі з втратами, тому дослідження цієї деталі також є актуальним.

2 МОДИФІКАЦІЯ МЕТОДУ ВИЯВЛЕННЯ ШТУЧНОГО ПІДВИЩЕННЯ РІЗКОСТІ

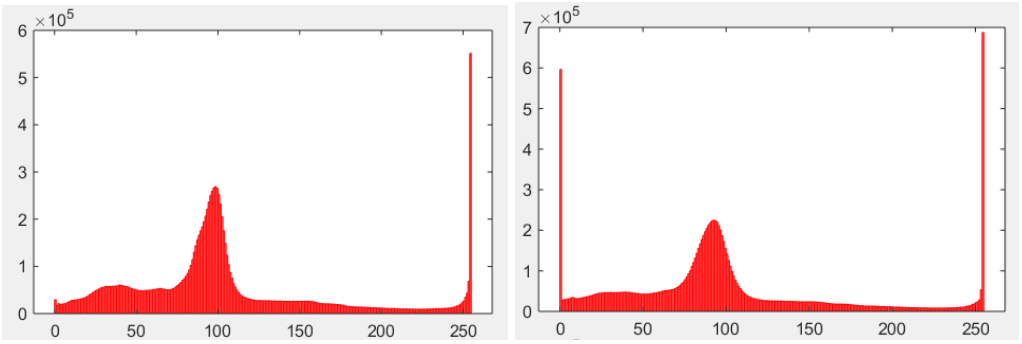
2.1 Основні положення методу виявлення штучного підвищення різкості

Не тільки професіонали, але й дилетанти на сьогоднішній день вміло застосовують засоби графічних редакторів для обробки фотографій. Спеціалізоване програмне забезпечення просте й інтуїтивно зрозуміле як серед платних графічних редакторів (наприклад, Adobe Photoshop), так і серед безкоштовних (наприклад, Gimp).

Обробка зображення різними фільтрами після його фальсифікації (розмиття, підвищенням різкості, корекція кольору, ретушування тощо) ускладнює виявлення фото підробок програмними засобами. Штучне підвищення різкості можна використовувати і для зловмисних намірів, наприклад для приховання фотомонтажу, або стеганографічна атака на зображення, і для побутових побажань, наприклад, досягнення певного художнього ефекту на фотографіях. Крім того, якщо мова йде про зловмисні наміри, застосування обробки має бути таким, аби воно не порушувало стійкість сприйняття цифрового зображення та не привертало уваги з боку експертів. Виявлення даного фільтру у цифровому зображенні свідчить про порушення його цілісності. Усе зазначене свідчить про актуальність теми.

В [13] було зазначено, що при застосуванні фільтру графічного редактора Gimp «Unsharp mask» у всіх трьох колірних компонентах цифрового зображення спостерігається значне збільшення пікселів зі значенням 0. 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 явище автори статті назвали «пік чорного».

Для автоматизації в роботі [13] запропоновано алгоритм, кроки якого наведемо далі.



а) б)

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

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 алгоритму полягає у порівнянні піку чорного з кількістю пікселів наступного за значенням кольору, тобто порівнянні 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 з втратами

Порівняння даного методу з іншими не можливе через брак даних за цією проблематикою. 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 [14] у форматі без втрат – спеціалізованої бази цифрових зображень прийнятної якості для проведення подібних експериментів, 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». Фільтр використано із параметрами за замовчуванням. Після обробки усі цифрові зображення було збережено у форматі з втратами (jpg). Для усіх цифрових зображень за трьома колірними компонентами було знайдено кількість пікселів зі значенням 0 до штучного підвищення різкості, та після нього. 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	60163	2,37685683
2	188507	512670	2,71963375
3	954	8996	9,42976939
4	47233	142776	3,02280185
5	35054	117192	3,3431848
6	22875	91609	4,00476503
7	10696	66025	6,17286836

Як можемо спостерігати, результати для червоної та зеленої компонент порівняні між собою і статистика за даними колірними компонентами така,

що можна виділити порогове значення для виділення оброблених зображень серед необроблених.

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	44243	2,69873124
2	82359	278508	3,38163407
3	28	3922	140,071429
4	16561	68570	4,14045046
5	8378	48409	5,77810933
6	195	28249	144,866667
7	7988	23088	2,8903355

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	2918944	0,74128829
2	240576	240576	2,36730181
3	3822	3822	6,93851387
4	1860674	1860674	0,65423712
5	3318235	3318235	0,688906
6	775796	4775796	0,70241317
7	6233357	6233357	0,70960351

Втім для синьої матриці даний ефект піку чорного не такий виражений. Про це свідчать результати експерименту. Тому використовувати синю колірну компоненту за даних обставин було б некоректно. Потрібні додаткові обстеження.

Для усіх оброблених зображень було проведено повторне застосування фільтру за тими ж параметрами. Результат повторної обробки збережено у форматі з втратами. 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	120312	1,9997673
2	572980	914096	1,78301051
3	10607	36421	4,04857715
4	162785	273052	1,91245027
5	136325	231106	1,97202881
6	109866	159161	1,7373948
7	83406	137215	2,07822794

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

Дане порогове значення визначено емпіричним шляхом. При даному значенні кількість помилок першого роду складає 6%, помилок другого роду – 13%.

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	87970	1,98833714
2	309015	512243	1,83923981
3	4555	7816	1,99286079
4	78881	139256	2,03085898
5	58510	90272	1,86477721
6	38140	53874	1,90711176
7	17769	37477	1,62322419

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	1893813	0,875234
2	602991	972887	1,7082698
3	31344	73833	2,7841548
4	1780279	839802	0,6898766
5	3281909	1749792	0,7654544
6	4783538	2659782	0,7928803
7	6285168	3569772	0,8070542

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

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

Зменшення порогового значення та отриманих показників у порівнянні з аналогічним експериментом для зображень, збережених після фальсифікації без втрат, зумовлене тим, що формат з втратами вносить певні артефакти у цифрове зображення. Один з основних кроків стиснення – квантування частотних коефіцієнтів у блоках матриці.

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	2,37685683	1,9997673
2	2,71963375	1,78301051
3	9,42976939	4,04857715
4	3,02280185	1,91245027
5	3,3431848	1,97202881
6	4,00476503	1,7373948
7	6,17286836	2,07822794

Отже, доцільно було б перевірити кількість 0-пікселів у блоках. Поставимо у відповідність зображенню так звану Матрицю нульових значень (МНЗ), кожен елемент якої відповідає блоку 8×8 та дорівнює кількості пікселів зі значенням 0 у даному блоці. Типовий вигляд даної матриці для зображення до обробки представлено на рисунку 2.1 у вигляді сукупності графіків для кожного рядка МНЗ, для зображень після обробки – на рисунку 2.2. Таке представлення дає змогу дивитись на матрицю в цілому. Перегляд матриці за елементами значно ускладнює аналіз через великі розміри зображень, що досліджувалися.

Якщо обчислити середнє значення для елементів даної матриці, то можна виділити порогове значення – 0,1. Дане порогове значення дозволяє відокремити оброблені цифрові зображення від необроблених.

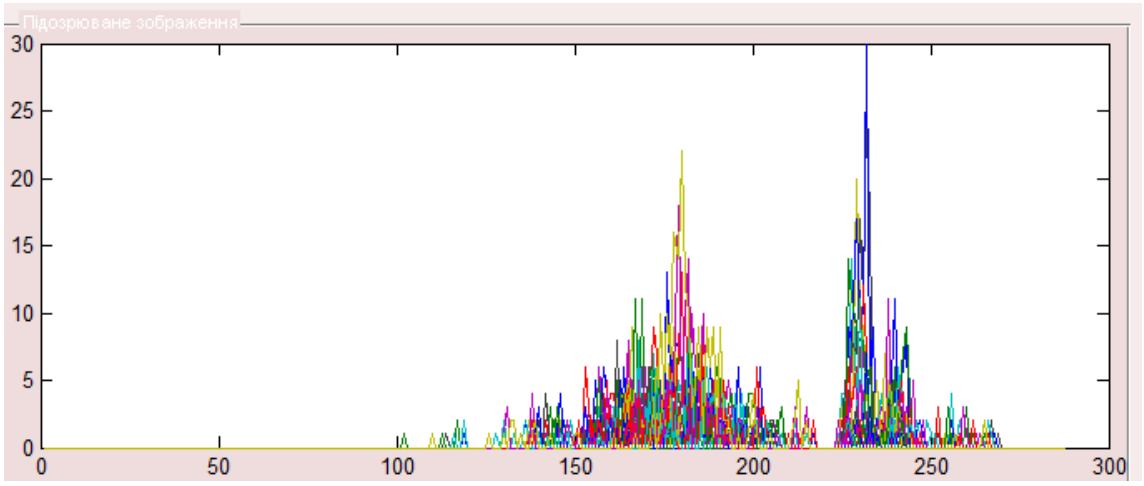


Рисунок 2.2 Графічне зображення МНЗ до обробки

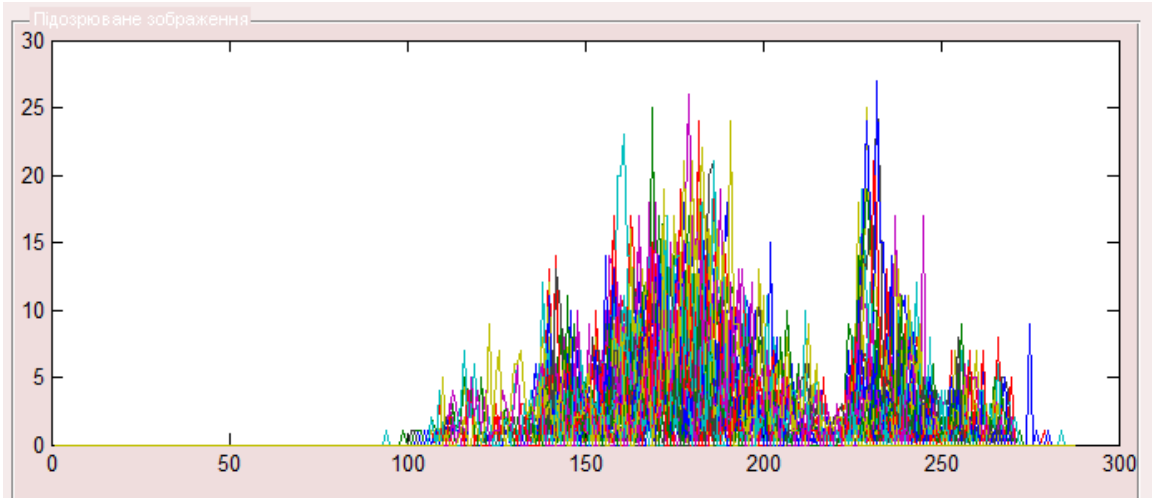


Рисунок 2.3 Графічне зображення МНЗ до обробки

Отримана також статистика помилок першого і другого роду. Встановлено, що помилки першого роду склали 8%, помилки другого роду – 10%. Результати даного підходу порівняні з результатами попереднього експерименту, тож можна віддати перевагу даному методу через можливість перевірити цифрове зображення без використання експертної обробки.

2.3 Модифікований метод

На основі проведених експериментів та отриманих результатів складемо алгоритм модифікованого методу виявлення штучного підвищення різкості цифрового зображення, збереженого у форматі з втратами після обробки.

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

1. Розбити матрицю R стандартним чином на блоки 8×8.
2. Для блоків матриці R знайти r_{ij}, що дорівнює кількості нульових значень у конкретному блоці.
3. Поставити матриці R у відповідність Матрицю нульових значень, кожен елемент якої відповідає блоку 8×8 і дорівнює кількості нульових значень в ньому.
4. Знайти середнє значення (K) елементів Матриці нульових значень.
5. *Якщо* $K<0,1$,

то зображення вважати не обробленим фільтром «Unsharp Mask»,

інакше виявлено штучне підвищення різкості.

У другому розділі проведено обчислювальний експеримент, на основі якого модифіковано метод виявлення штучного підвищення різкості та розроблено його алгоритм.

3 РЕАЛІЗАЦІЯ МОДИФІКОВАНОГО МЕТОДУ

Для реалізації модифікованого методу добре зарекомендувало себе середовище MATLAB. Дане середовище має потужні бібліотеки математичних та статистичних функцій, підтримує об’єктно-орієнтований інтерфейс.

Для проведення описаних експериментів було використано функції математичного і графічного моделювання Matlab. Основні переваги середовища Matlab вигідно виділяють її серед існуючих нині математичних систем і пакетів (MathCad, Mathe- matica і ін.). Система Matlab спеціально створена для проведення саме інженерних розрахунків: математичний апарат, який використовується нею, гранично наближений до сучасного математичного апарату інженера і вченого і спирається на обчислення з матрицями, векторами і комплексними числами; графічне представлення функціональних залежностей тут організовано у формі, необхідній для створення інженерної документації.

Завантажувати зображення будемо до об’єкту axis. На відміну від модифікованого методу для зображень без втрат у даній модифікації необхідним є лице підозрюване зображення без додаткової обробки експертом.

Також для зручності завантаження нових зображень та коректної роботи програми передбачимо кнопку очищення об’єкту axis від зображень. Реалізуємо також кнопку виходу з застосунку.

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 програмного продукту. 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.

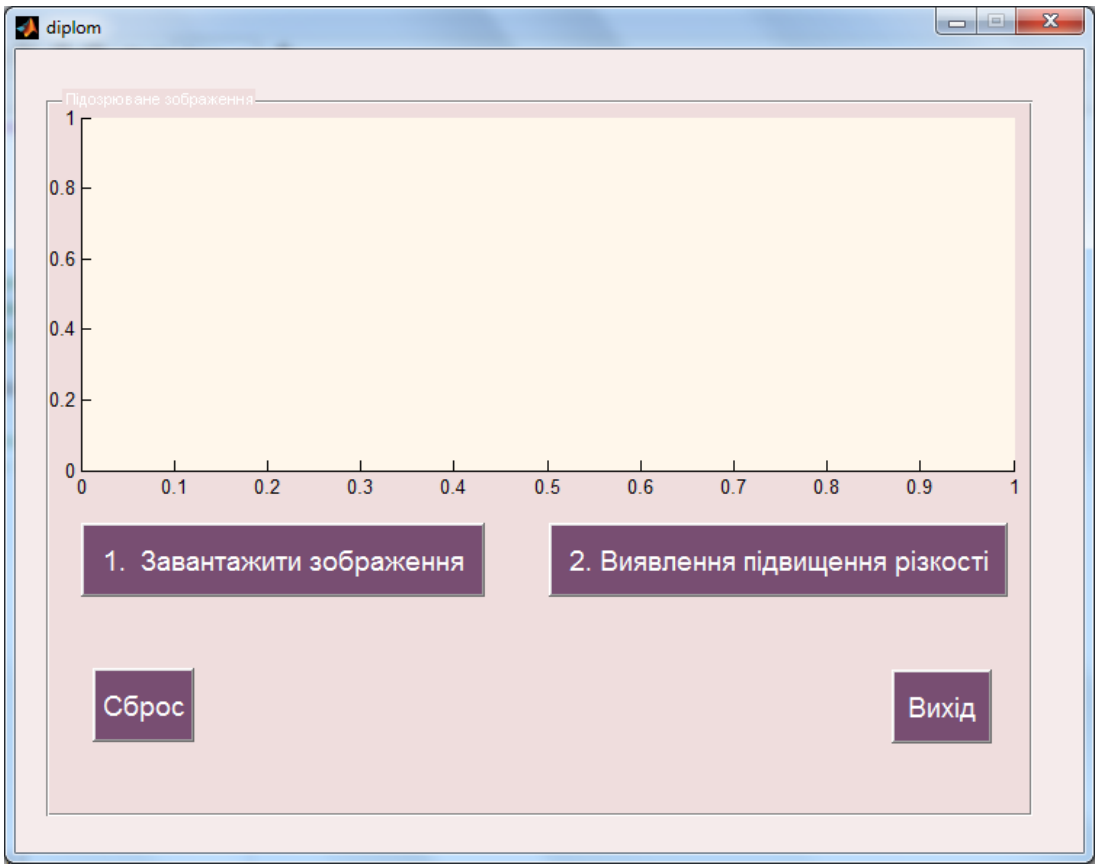


Рисунок 3.1 Інтерфейс програмного продукту

При натисканні кнопки 1 зявляється вікно вибору зображення (рис.3.2).

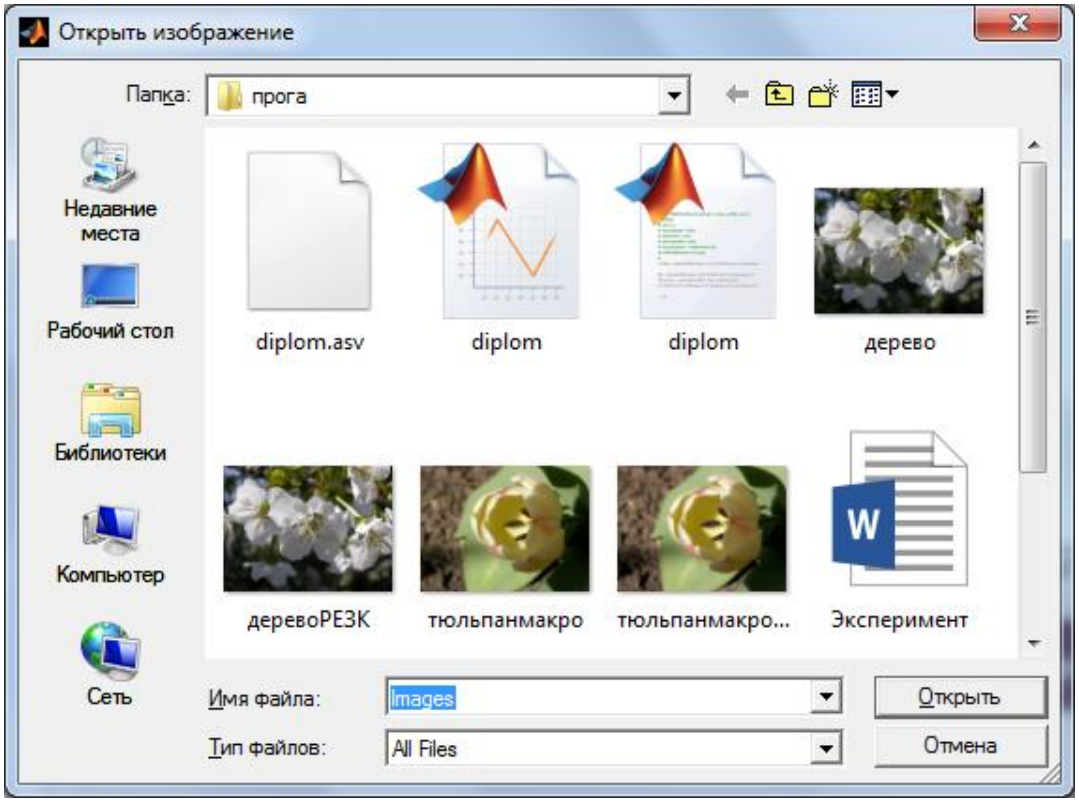


Рисунок 3.2 Вікно вибору зображення для перевірки

Розглянемо програмний код кнопки «Завантажити зображення». Його наведено на рисунку 3.3.

```
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 3.3 – Програмний код кнопки «Завантажити зображення».

Після вибору зображення можемо бачити об’єкт перевірки у вікні інтерфейсу (рис.3.4).

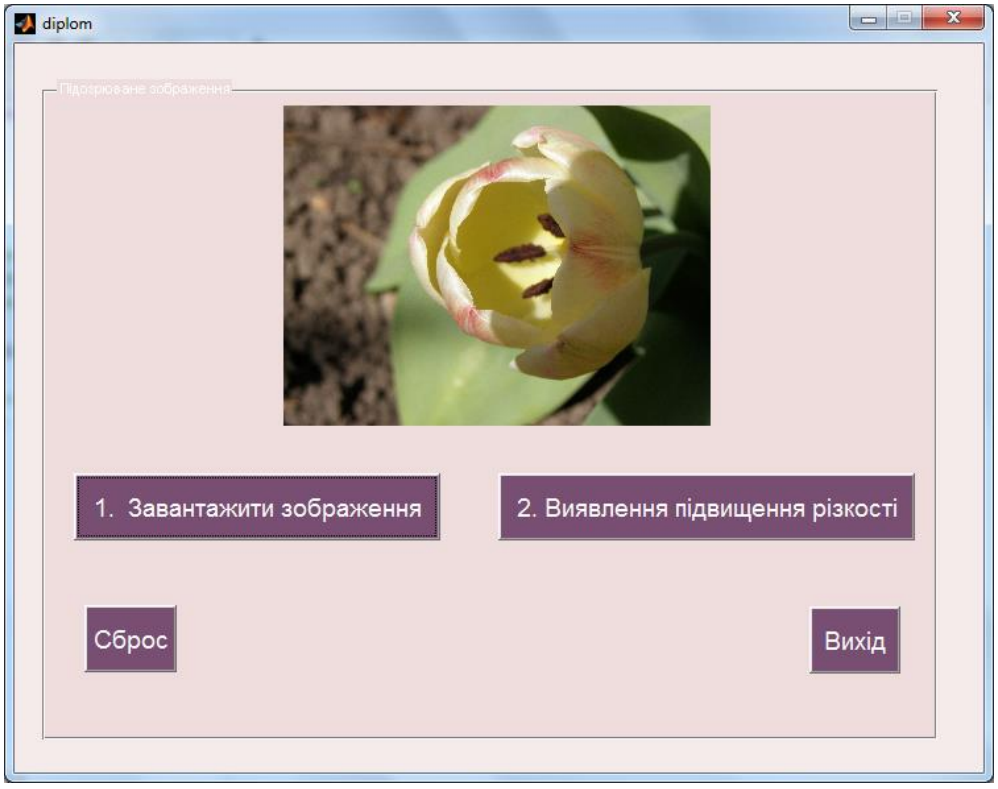


Рисунок 3.4 Завантаження зображень для перевірки

Наступний крок – застосування кнопки 2 «Виявлення підвищення різкості». Дана кнопка містить декілька блоків програмного коду. Перший блок – перехват глобальної змінної у вигляді цифрового зображення для перевірки та виділення червоної колірної компоненти для подальшого аналізу (рис.3.5).

Другий блок – побудова Матриці нульових значень (рис.3.6). Третій завершальний блок – розрахунок середнього значення Матриці нульових значень та порівняння його з пороговим значенням (рис.3.7).

```
T{1}=handles.Image1;
IZ=double(T{1});
IZR=IZ(:,:,1);
n=fix((size(IZR,1))/8)*8;
m=fix((size(IZR,2))/8)*8;
IZR=IZR(1:n,1:m);
```

Рисунок 3.5 Виділення матриці для аналізу

```
MNul = blkproc(IZR,[8 8],'length(find(x<1))');
KoefBlack=mean(mean(MNul));
```

Рисунок 3.6 Побудова Матриці нульових значень

```
if KoefBlack>0.1
helpdlg('Виявлено штучне 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 «Виявлення підвищення різкості» виконується обробка завантаженого цифрового зображення та 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».

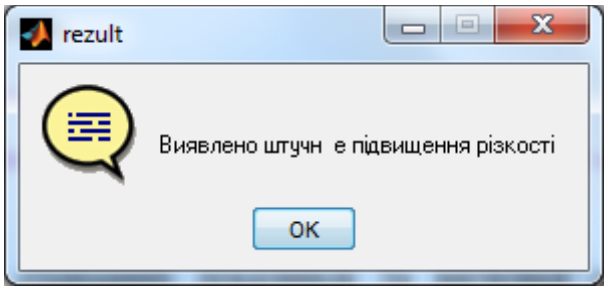


Рисунок 3.8 Результат перевірки цифрового зображення

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

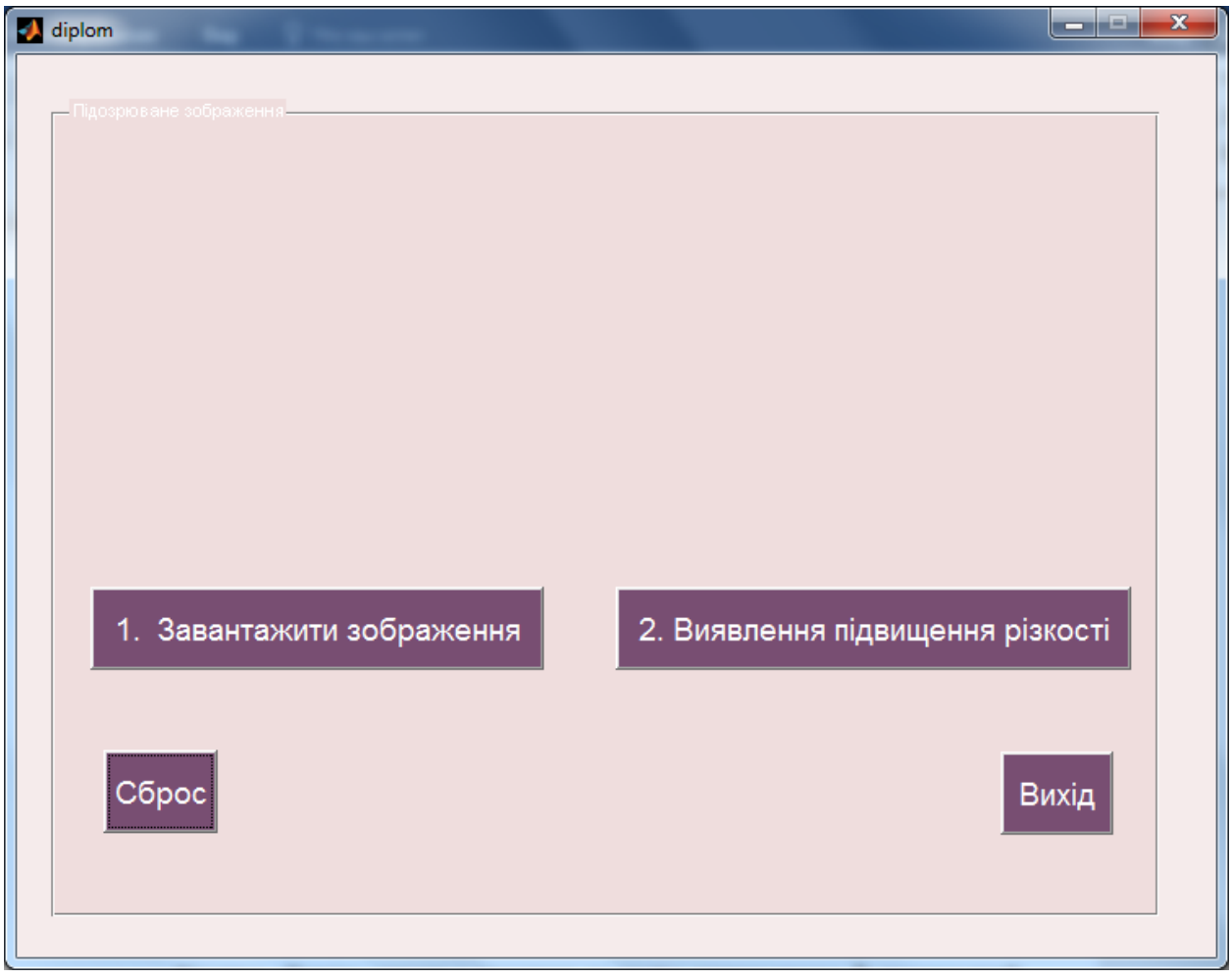


Рисунок 3.9 Очищення від завантаженого зображення

Програмний код цієї кнопки наведено на рисунку 3.10. Даний результат отримуємо шляхом застосування функції cla.

```
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».

Оскільки цифрові зображення для експерименту було оброблено засобами графічного редактора GIMP, продемонструємо процес підготовки до дослідження. Дану процедуру будемо демонструвати з міркувань того, що отримані результати мають бути повторюваними. Тож якщо виникне необхідність, можна буде використовувати цю частину як опору. 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).

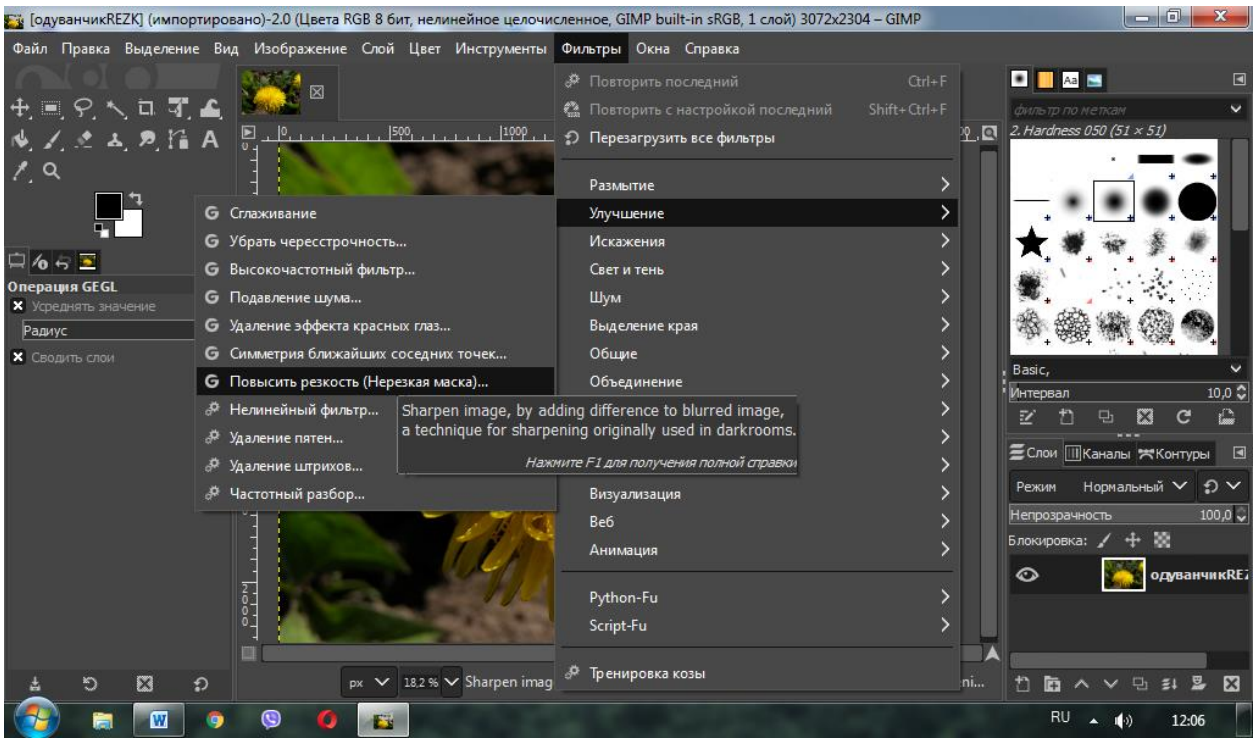


Рисунок 3.12 Пошук фільтру для обробки зображення

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.

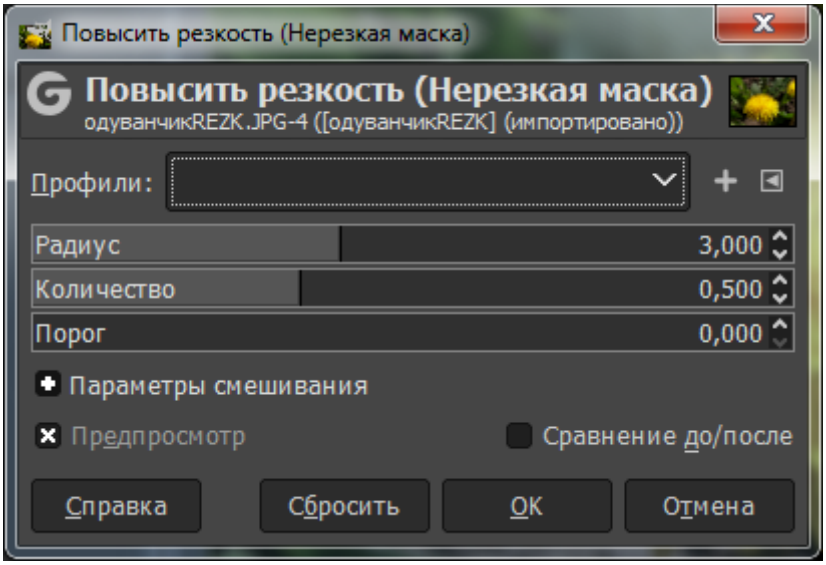


Рисунок 3.13 Настроювані параметри фільтру штучного підвищення різкості

Зміна даних параметрів призведе до підвищення описаного в роботі ефекту, 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 було використано 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 з втратами jpg, 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 вважати таким, що містить сліди порушення його цілісності у вигляді штучного підвищення різкості. Дане порушення можна виявити засобами розробленого програмного застосунку.

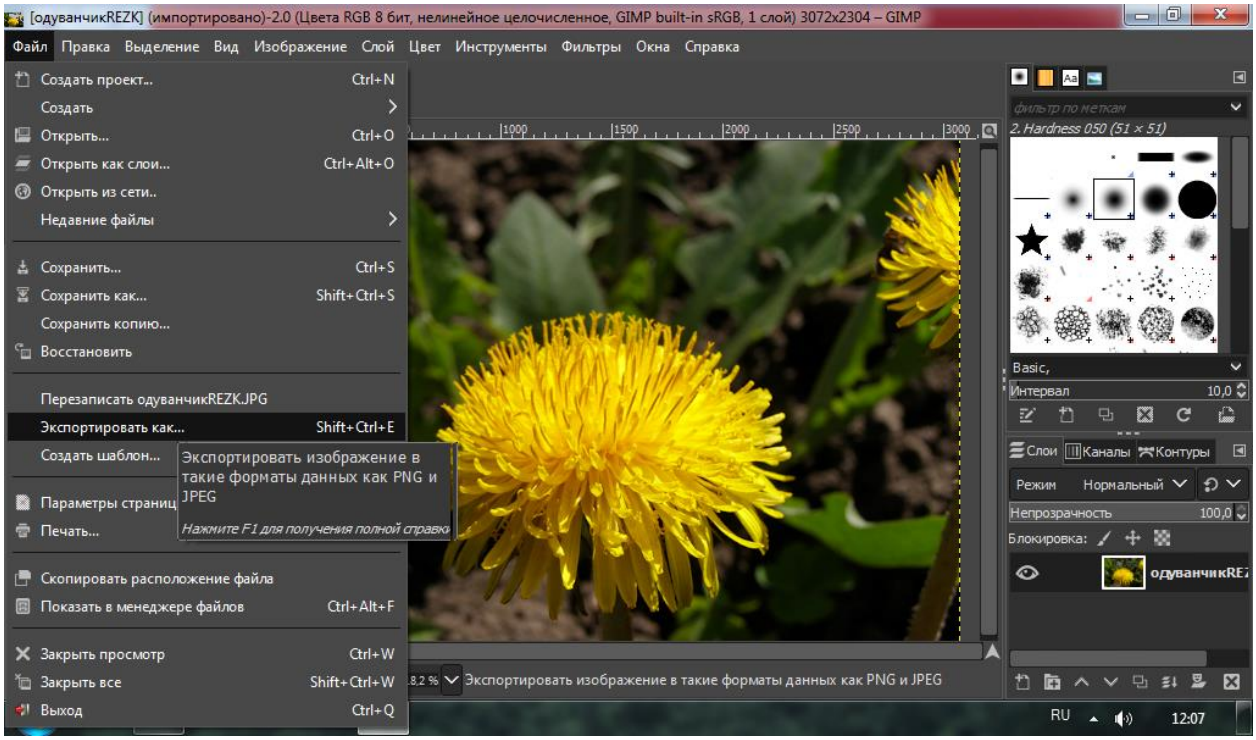


Рисунок 3.14 – Збереження файлу після його обробки

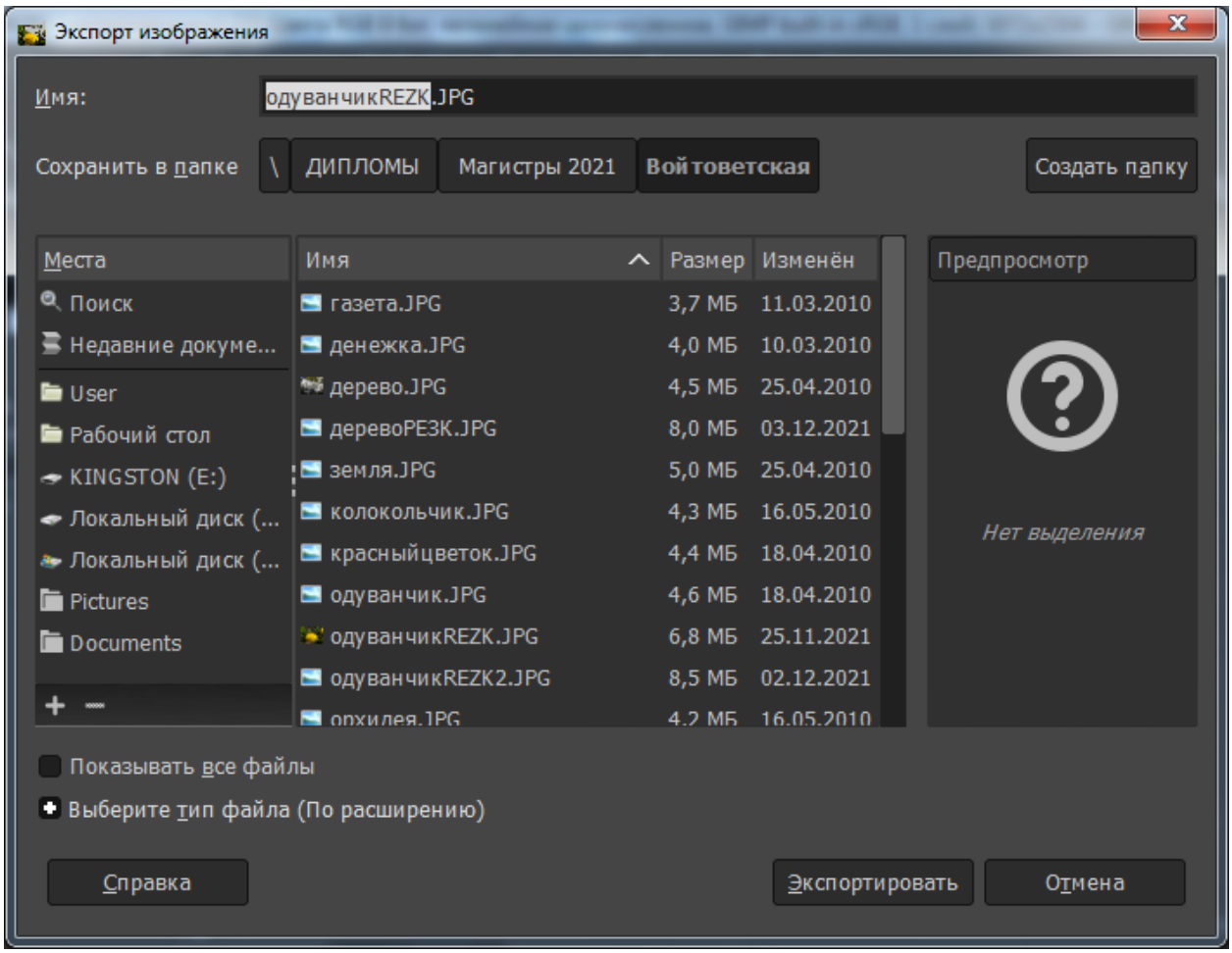


Рисунок 3.15 Налаштування параметрів збереження

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 без втрат. Також можна доповнити даний за стосунок іншими методами, направленими на пошук таких порушень цілісності, як розмиття, клонування, масштабування тощо.

Можливо також виконати адаптацію даного програмного продукту для використання на мобільних пристроях.

4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів. Охорона праці – це комплексна система заходів і засобів, які призначені зберігати життя і здоров'я людини під час її трудової діяльності. Основні законодавчі акти з охорони праці це: Конституція України, яка гарантує кожному громадянину його права; Закон України про охорону праці, який визначає основні положення щодо реалізації конституційного права громадян на охорону життя і здоров'я у процесі трудової діяльності і встановлює єдиний порядок організації охорони праці в Україні; Кодекс законів про працю, який регулює трудові відносини працівників і працедавців. Основні нормативні документи з охорони праці: державні стандарти України, державні будівельні норми і правила, санітарні норми і правила, які стосуються вимог щодо окремих компонент виробничого середовища (параметрів мікроклімату, освітленості, рівнів шуму, рівнів інтенсивності іонізуючих і електромагнітних випромінювань, електричного обладнання, а також ергономічних характеристик робочого місця).

Заходи і засоби захисту від небезпечних і шкідливих виробничих факторів (НШВФ) для конкретного робочого місця обирають, виходячи із аналізу умов праці і трудового процесу. В свою чергу, аналіз умов праці полягає у зіставленні фактичних значень НШВФ із нормативними і оцінюванні перевищення, якщо таке виявлене, за певними критеріями.

На перший погляд, на робочому місці програміста, оснащеному офісною технікою та комп'ютерами, відсутні фактори виробничої небезпеки або шкідливі фактори, здатні вплинути на здоров'я працівників. Однак уважний аналіз умов праці за стандартними алгоритмами [15] дозволяє визначити суттєву кількість небезпечних і шкідливих виробничих факторів, а саме:

– підвищену влітку або знижену взимку температуру повітря робочої зони, підвищену вологість повітря робочої зони: це явище можливе при нехтуванні системами нормалізації параметрів повітря;

– підвищений рівень іонізації позитивними іонами, який виникає внаслідок роботи дисплейних пристроїв і принтерів;

– підвищену запиленість повітря робочої зони, яка виникає внаслідок нехтування вимогами щодо прибирання приміщення із комп'ютерами і підвищеного вмісту позитивних іонів в повітрі, а також внаслідок інтенсивного друку лазерними принтерами;

– підвищений рівень шкідливих речовин в повітрі робочої зони внаслідок інтенсивного друку лазерними принтерами (частинки тонерів) і при значному нагріванні елементів комп'ютерів, виготовлених з пластику (корпусів);

– підвищений рівень шуму на робочому місці, який виникає внаслідок використання потужних персональних комп'ютерів, принтерів, іншого обладнання;

– підвищений рівень вібрації на робочому місці, який виникає внаслідок використання потужних персональних комп'ютерів, принтерів, іншого обладнання;

– підвищену напругу в електричних мережах із імовірністю замикання на тіло працівника, внаслідок чого людина набуває загальної травми – електричного удару, і місцевих травм – опіків;

– недостатній рівень освітленості робочих поверхонь, який виникає внаслідок помилок в розміщенні робочих місць відносно світильників і вікон;

– імовірність механічних травм внаслідок падіння працівника з вишини свого зросту при невдалому розміщенні робочих місць, якщо він чіпляється за дроти і меблі при нестачі вільного простору;

– імовірність механічних травм внаслідок падіння працівника з вишини більше свого зросту при невдалому розміщенні шаф із документами і

необхідними матеріалами, якщо він користується драбиною або не призначеними для цього предметами для того, щоб дістатися їх;

– достатньо високий рівень пожежної небезпеки, чому слід приділити окремої уваги.

Таким чином, оскільки на робочому місці наявний вплив достатньо великої кількості небезпечних і шкідливих виробничих чинників на працівника, вимоги охорони праці під час роботи з комп'ютером охоплюють не тільки сам процес праці, а й обставини, що супроводжують його, тобто умови праці, які також впливають на працездатність і збереження здоров'я співробітника Вони являють собою перелік вимог, які стосуються наступних аспектів:

– вимоги до приміщень, у яких виконується робота із застосуванням персональних комп'ютерів;

– загальні правила організації праці з використанням комп'ютерної та офісної техніки;

– вимоги до персонального комп'ютера, який використовується як основне виробниче обладнання для постійної роботи працівника;

– вимоги до електробезпеки виробничого обладнання;

– вимоги до повітря робочої зони стосовно мікроклімату для відповідних робочих місць, а також стосовно вмісту у повітрі робочої зони позитивних і негативних аероіонів, пилу та шкідливих речовин;

– вимоги щодо рівню шуму, що генерується виробничим обладнанням;

– вимоги щодо рівню вібрації, що генерується виробничим обладнанням;

– вимоги щодо організації освітлення робочої зони;

– вимоги щодо медичного контролю за здоров'ям персоналу;

– вимоги щодо порядку організації державного санітарно-епідеміологічного нагляду та виконання виробничого контролю.

Для розміщення робочих місць програмістів обирають приміщення офісного типу. В приміщенні може бути від одного окремого робочого місця

до великої їх кількості, так званих опен офіс – приміщень із відкритим виробничим простором. Для визначення допустимої кількості робочих місць користуються умовою, що на одне робоче місце слід розраховувати мінімально 6,0 $м^2$ вільної площі приміщення і мінімально 20,0 $м^3$ вільного об'єму приміщення [16]. Взаємне розташування робочих місць в приміщенні також регламентується. Незалежно від кількості, робочі місця повинні бути розміщені на відстані не менше ніж 1 м від стіни з віконними перерізами і на відстані не менше ніж 1,4 м від стіни без віконних перерізів. Між бічними поверхнями моніторів комп'ютерів слід дотримуватися відстані не менше 1,2 м; відстань між задньою поверхнею одного монітора та екраном іншого повинна бути не менше 2,5 м [16].

В приміщеннях слід передбачати природне освітлення і системи штучного освітлення. Для забезпечення достатнього рівня природного освітлення слід обирати приміщення із великими вікнами, орієнтованими оптимально на північ або схід. Коефіцієнт природної освітленості повинний бути не менше 1,5 % [16].

Системи штучного освітлення складаються з світильників загального освітлення, розміщених на стелі або стінах у вигляді суцільних або переривчастих ліній, і світильників місцевого освітлення, розташованих безпосередньо на робочих столах. В якості джерел світла загального освітлення слід застосовувати люмінесцентні або світлодіодні лампи. В якості джерел світла місцевого освітлення слід застосовувати переважно світлодіодні лампи, але допускається використання ламп накалювання. Лампами, не встановленими у світильники, користуватись заборонено.

В приміщеннях із комп'ютерами рекомендовано застосовувати світильники прямого світла – клас світлорозподілу П, і світильники переважно відбитого світла – клас світлорозподілу В. Світильники обох типів слід обладнати розсіювачами і екранами. Застосування світильників без розсіювачів та екранів заборонено.

Системи освітлення повинні створювати на поверхнях робочого місця нормоване значення освітленості не менше 500 лк. Для обмеження прямої блискості від джерел природнього та штучного освітлення яскравість вікон і джерел світла, що опиняються у полі зору працівника, повинна бути не більше 200 кд/м^2. Світильники слід оздоблювати розсіювальними елементами, вікна слід закривати фіранками або жалюзі [16].

Оскільки імовірність ураження електричним струмом є основною травмостворюючою небезпекою, вимоги електробезпеки при використанні комп'ютерів поширюються на обладнання і процеси його використання.

Перед початком роботи за комп'ютером слід виконати наступні операції:

– перевірити справність елементів живлення комп'ютера і оргтехніки, в тому числі електропроводки, вимикачів, вилки та розетки, за допомогою яких необхідна апаратура підключається до мережі;

– проконтролювати стан заземлення комп'ютера і перевірити його працездатність.

У процесі роботи слід дотримуватись наступних правил:

– забороняється класти на корпус комп'ютера і оргтехніки сторонні предмети, торкатися їх мокрими руками, проводити чищення корпусу обладнання, яке знаходиться під напругою;

– у разі виявлення несправності комп'ютера слід негайно припинити роботу та повідомити про це безпосереднього керівника;

– експлуатувати комп'ютери слід лише із дотриманням інструкції, наданої виробником;

– необхідно уникати частого та необґрунтованого включення та вимикання комп'ютера під час роботи.

Після закінчення роботи за комп'ютером його слід вимкнути за алгоритмом, встановленим виробником, знеструмити периферійне обладнання и переконатися у відключенні техніки. Після цього слід вимкнути рубильники електроживлення в виробничому приміщенні.

Режими праці та відпочинку мають велике значення для збереження здоров’я працівників. Тривалість періодів праці та відпочинку для персоналу, що постійно працює із комп’ютерами і оргтехнікою, регламентована на законодавчому рівні. При 8-годинному робочому дні в залежності від тяжкості та напруженості праці загальна тривалість перерв на відпочинок має становити від 50 до 90 хвилин. Проводити перерви на відпочинок сидячи за комп’ютером, витрачаючи їх на читання новин або онлайн-ігри, не можна. Необхідно під час перерв виконувати фізичні вправи, гімнастику для очей, зробити коротку прогулянку на відкритому просторі. Тривалість перерв на відпочинок згідно з чинним трудовим законодавством враховується в загальну тривалість робочого дня. Тривалість робочого дня не збільшується за рахунок періодів відпочинку. Також у час перерв на відпочинок працівника заборонено залучати до іншої трудової діяльності, оскільки це вже не буде вважатися відпочинком. Стандартний час для обіду додається до перерв на відпочинок окремо.

Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях. Техногенна небезпека – стан, внутрішньо властивий технічній системі або об’єкту, який 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.

Основною техногенною небезпекою в приміщеннях із персональними комп’ютерами і оргтехнікою є пожежі.

Основні причини виникнення пожеж:

– порушення вимог електробезпеки під час експлуатації персональних комп’ютерів і оргтехніки;

– пошкодження засобів колективного захисту від ураження електричним струмом, або їх відсутність;

– підключення персональних комп’ютерів і оргтехніки до пошкоджених елементів електромережі: розеток, проводів із пошкодженою ізоляцією;

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

– нагромадження паперових документів на корпуси обчислювальної техніки;

– використання на робочому місці електронагрівальних пристроїв, побутової техніки та іншого обладнання, що не належить до обчислювальної технікі; їх підключення в електромережу через пристрої, не призначені для обладнання великої потужності, а саме через мережеві фільтри, блоки безперебійного живлення і спеціалізовані розетки;

– куріння в непристосованих для цього місцях (на робочому місці).

Для забезпечення електробезпеки і пожежовибухобезпеки необхідно використовувати персональні комп’ютери, периферійні пристрої і оргтехніку, які мають виконання та ступень захисту у відповідності до вимог ПУЕ [17]. Підключати вказану техніку слід із використанням апаратури захисту від перевантаження, стрибків напруги, короткого замикання та інших аварійних режимів.

Засоби колективного захисту, які використовують в приміщеннях із персональними комп’ютерами: захисне штучне заземлення, захисне занулення, пристрої захисного відключення.

В кожному приміщенні із комп’ютерною технікою необхідно розміщати вуглекислотні або порошкові вогнегасники із розрахунку один вогнегасник на кожні 50 $м^2$ площі приміщення, але не менш ніж один вогнегасник на приміщення. Вогнегасники слід розміщати в помітних і легкодосяжних місцях, захищених від прямих сонячних променів і механічних впливів (штовхань, ударів). Кожен вогнегасник повинний мати сертифікат якості. Працівники обов’язково мають пройти навчання щодо правил експлуатації вогнегасників.

Проектування системи загального штучного освітлення. З метою створення безпечних і комфортних умов праці, особливо зорової і розумової праці, приміщення із робочими місцями працівників інформаційної галузі обов'язково обладнують системами комбінованого штучного освітлення.

Вихідні дані для проектування системи штучного освітлення:

– фактична освітленість на робочих місцях (на поверхні столу), виміряна за допомогою люксметра: $E_ф$ = 180 лк;

– розміри приміщення: довжина A = 26 м; ширина B = 20 м;

– розрахункова висота підвісу світильників: H = 4,0 м;

– найменший розмір об'єкта розрізнення: 0,5 мм;

– контраст об'єкта розрізнення з фоном – великий

– характеристика фону – світлий;

– концентрація пилу в повітрі: 0,5 мг/м^3;

– коефіцієнти відображення: 0,7 – 0,5 – 0,3.

Розряд зорової роботи в даному приміщенні обираємо: III розряд, роботи підвищеної точності [17]. Для III розряду зорової роботи задана норма освітленості на робочому місці: $E_н$ = 450 лк. Таким чином, фактична освітленість на робочих місцях $E_ф$ = 180 лк значно менша за нормативну освітленості $E_н$ = 450 лк. Для даного приміщення є потреба в модернізації системи освітлення.

Для загального освітлення обираємо світильники моделі ЛВП02-4Х80, призначені для встановлення чотирьох люмінесцентних ламп потужністю до 80 Вт. Люмінесцентні лампи застосовують в приміщеннях з підвищеними вимогами до передачі кольору, що відповідає умовам зорової роботи високої точності і при розміщенні світильників на висоті до 4 м.

Площа приміщення:

$$S = AB = 26 \cdot 20 = 520 \text{ м}^2$$

Індекс приміщення:

$$i = \frac{S}{(A+B)\cdot H} = \frac{520}{(26+20)\cdot 4,0} = 2,83$$

Еквівалентна площа:

$$S_e = \frac{S \cdot K \cdot z}{\eta} = \frac{520 \cdot 1,3 \cdot 0,4}{0,33} = 820 \text{ м}^2.$$

Попередня розрахункова кількість світильників:

$$N_o = \frac{S}{L_o^{\,2}} = \frac{520}{3,5^2} = 43 \text{ шт.}$$

Приймаємо $N_o = 45$ шт.

Потрібний світовий потік світильника:

$$\Phi_c = \frac{S_e \cdot E_н}{N_o} = \frac{820 \cdot 450}{45} = 8200 \text{ лм.}$$

Освітленість E_1, яка створюється одним світильником:

$$E_1 = \frac{n \cdot \Phi}{S_e} = \frac{4 \cdot 8200}{820} = 40 \text{ лк.}$$

Кількість світильників:

$$N_n = \frac{E_н}{E_1} = \frac{450}{40} = 11,4 \text{ шт.}$$

Приймаємо остаточну кількість світильників для монтажу $N = 12$ шт.

Таким чином, в приміщенні із персональними комп'ютерами довжиною 26 м і шириною 20 м необхідно встановити на стелі 12 світильників моделі ЛВП02-4Х80, оснащених чотирма люмінесцентними лампами. Світильники оптимально рівномірно розташувати на стелі в три ряди. Додатково до світильників загального освітлення слід розмістити на робочих столах настільні світлодіодні світильники місцевого освітлення.

ВИСНОВКИ

В роботі проведено аналіз джерел з виявлення порушень цілісності цифрового зображення. Було встановлено, що проблема виявлення фальсифікацій 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 два обчислювальні експерименти з використанням 600 цифрових зображень. Усі зображення було оброблено фільтром фоторедактору GIMP «Unsharp Mask» та збережено у форматі з втратами.

Отримано порогове значення (2) для застосування експертної обробки при збереженні зображення у форматі з втратами. Кількість помилок першого і другого роду при даному підході становила 6 і 13 відсотків відповідно.

Було встановлено порогове значення (0,1) для відділення оброблених цифрових зображень від необроблених при застосуванні підходу, заснованого на аналізі кількості нульових чисел блоків матриці цифрового зображення. Кількість помилок першого і другого роду при даному підході становила 8 і 10 відсотків відповідно.

На основі проведених експериментів та отриманих результатів було модифіковано метод, реалізовано його алгоритм. Модифікований метод реалізовано у програмному середовищі Matlab. Програмний продукт є простий у використанні, має інтуїтивно зрозумілий інтерфейс та виконує усі необхідні для перевірки функції.

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*.. С. 56-62.

2. Parry Z. Digital manipulation and photographic evidence*:* defrauding the courts one thousand words at a time. *Journal of Law, Technology & Policy*. 2009. P.175-202.

3. Magar S. Ultra-diluted Toxicodendron pubescens attenuates pro-inflammatory cytokines and ROS-mediated neuropathic pain in rats. *Scientific Reports.* 2018. №8. P.1-11.

4. Guglielmi G. Peer-reviewed homeopathy study sparks uproar in Italy. *Nature*. 2018. №562. P.173-174.

5. Schneider L. Who cures cancer in Photoshop? *URL: https://forbetterscience.com/2018/10/11/who-cures-cancer-in-photoshop/*

6. Gilbert N. Science journals crack down on image manipulation. *URL: https://www.nature.com/articles/news.2009.991/box/1*

7. Brainard J, You J. What a massive database of retracted papers reveals about science publishing's 'death penalty'. *Science*. 2018. №10. P.189-194.

8. Sophie J. Nightingale, Kimberley A. Wade & Derrick G. Watson Can people identify original and manipulated photos of real-world scenes? *Cognitive Research: Principles and Implications.* 2017. №2. P.30

9. Kumar B.S., Karthi S., Karthika K., Cristin R. A Systematic Study of Image Forgery Detection. *Journal of computational and theoretical Nanoscience*. 2018. №15(8). P.2560–2564.

10. Garnett R., Huegerich T., Chui C., He W. A Universal Noise Removal Algorithm with an Impulse Detector. *IEEE Trans Image Proccess*. 2005. №14(11). P.1747-1754.

11. Сорокин С.В., Щербаков М.А. Реализация SD-ROM фильтра на основе концепции нечеткой логики. *Известия высших учебных заведений. Поволжский регион.* 2017. №3. С.56-65.

12. Красовский Г.Я., Усс М.Л. Фильтрация изображений, искаженных импульсными помехами точечного и строчного типа, на основе систем итерированых функций. *Радіоелектронні і комп'ютерні системи*. 2003. №2. С.47-55.

13. Chan R., Ho C., Nikolova M. Salt-and-pepper noise removal by median-type noise detectors and detail preserving regularization. *IEEE Trans. Image Proc*. 2005. №14(10). P.1479-1485.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.

14. NRCS Photo Gallery. United States Department of Agriculture. Washington, USA. URL: http://photogallery.nrcs.usda.gov

15. Постанова Кабінету Міністрів України «Про Порядок проведення атестації робочих місць за умовами праці» №442 від 1.08.1992 р.

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

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