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

Козаченко Наталія Геннадіївна,
студентка групи РФ-161

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Модифікація алгоритму виявлення результатів масштабування цифрового зображення

Спеціальність:
122 Комп’ютерні науки

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 122 – Комп'ютерні науки

Освітня програма – Програмне забезпечення систем захисту інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри КБПЗ

_____

д.т.н.,проф. А.А.Кобозєва

____ _____2021р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Козаченко Наталії Геннідіївні

1.Тема роботи: *Модифікація алгоритму виявлення результатів масштабування цифрового зображення.*

керівник роботи *Зоріло Вікторія Вікторівна, к. т. н.,*

затверджені наказом ректора ДУОП від „25" жовтня 2021 р. № 372-в.

2.Зміст роботи*: огляд підходів та методів вирішення проблеми виявлення порушень цілісності цифрового зображення, модифікація алгоритму виявлення масштабування, 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 _____ *Козаченко Н.Г.*

Керівник роботи _____ *Зоріло В.В.*

ЗАВДАННЯ
на розробку розділу «Охорона праці»

Козаченко Наталії Генадіївні, група РФ-161

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Тема роботи *Модифікація алгоритму виявлення результатів масштабування цифрового зображення.*

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. Освітлення робочого місця інженера-програміста.

Керівник роботи
_____ (В.В. Зоріло)
«____» _____ 2021 р.

Консультант з охорони праці
_____ (_____)
«____» _____ 2021 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему «Модифікація алгоритму виявлення результатів масштабування цифрового зображення» на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 122 – Комп'ютерні науки, спеціалізація, освітня програма: Програмне забезпечення систем захисту інформації виконана в обсязі 58 сторінок і містить 16 рисунків, 1 таблицю та 38 джерел за переліком посилань.

Метою роботи є підвищення ефективності виявлення масштабування як порушення цілісності цифрового зображення.

Методи досліджень базуються на використанні загального підходу до аналізу стану та технології функціонування інформаційної системи, а також на статистичному аналізі та матричному аналізі.

Модифіковано алгоритм виявлення масштабування як порушення цілісності цифрового зображення. Виконана модифікація дозволила знизити кількість хибних тривог при аналізі зображень.

Результати роботи можуть бути використані судовими лабораторіями та експертами-криміналіста при перевірці цифрових зображень на наявність в них фальсифікації.

ЦИФРОВЕ ЗОБРАЖЕННЯ, СИНГУЛЯРНІ ЧИСЛА, МАСШТАБУВАННЯ.

ANNOTATION

Qualification work on "Software development for the comprehensive verification of digital images for violations of their integrity" for the first

(bachelor's) level of higher education in the specialty 125 – Cybersecurity, specialization, educational program: Cybersecurity is 58 pages and contains 16 figures, 1 table and 38 sources according to the list of references.

The aim of the work is a comprehensive inspection of digital images for damage to their integrity.

Research methods are based on the use of a general approach to the analysis of the state and technology of the information system, as well as statistical analysis and matrix analysis.

Software has been developed that includes three algorithms for detecting integrity violations, such as cloning, scaling, and blurring. The interface for using these algorithms is convenient and easy to use.

The results can be used by forensic laboratories and forensic experts to check digital images for falsification.

Possible areas of further research are the continuation of work on the analysis of the impact of various types of unauthorized interference in the digital image in order to change its content and meaning.

DIGITAL IMAGE, SINGULAR NUMBERS, SCALING.

ЗМІСТ

ВСТУП

Актуальність теми. У вік інтенсивного розвитку і впровадження в усі сфери діяльності людини інформаційних технологій особливо гостро ставиться питання захисту інформації. Про це свідчать останні події у світі: інформаційні війни, що ведуться урядами країн під час політичних конфліктів, можуть мати непередбачувані наслідки для населення. Велику роль у сучасному світі відіграють цифрові сигнали, зокрема, цифрові зображення (ЦЗ), що використовуються у науці, медицині, судових розглядах, пресі і т.д. Через загальнодоступність програмного забезпечення, що дозволяє обробляти і редагувати ЦЗ, а також у зв'язку з різноманітністю способів їх фальсифікації, зростає необхідність у вдосконаленні існуючих та розробці нових методів виявлення порушення цілісності ЦЗ, що є обов'язковою складовою частиною будь-якої сучасної комплексної системи захисту інформації.

Даним напрямком займаються вчені всього світу, і все ж існуючі сучасні розробки для виявлення порушень цілісності цифрових зображень при всьому їх різноманітті не завжди є ефективними, мають суттєві недоліки.

Так, багато сучасних методів засновані на використанні цифрових водяних знаків, проте через відсутність можливості попередньої вбудови цифрових водяних знаків у більшості технічних засобів генерації цифрового

відео та зображення використання даних методів часто є неможливим.

З відкритого доступу відомо про методи виявлення фальсифікації ЦЗ, засновані на аналізі exif-даних. Але, використання даних методів не дає можливості локалізації області фальсифікації ЦЗ, а лише констатує факт його можливого редагування; існують програмні засоби редагування exif-даних, застосування яких взагалі приводе до неможливості використання даних методів.

Активно розвиваються наразі методи виявлення фальсифікацій цифрових зображень, засновані на загальному підході до аналізу стану та технології функціонування інформаційних систем. Серед цих методів деякі направлені на виявлення фальсифікації, виконаної шляхом комбінації різних цифрових зображень, деякі виявляють фальсифікації на основі клонування, також є методи, спрямовані на виявлення пост обробки цифрового зображення після його фальсифікації.

Існуючі методи виявлення фальсифікацій цифрового зображення, як правило, не дієздатні при малому розмірі фальсифікованої області (зокрема, коли ця область має розміри блока, отриманого при стандартному розбитті матриці зображення), хоча саме такі області дуже часто використовуються в процесі фальсифікацій; найефективнішим у виявленні клонування цифрового зображення є метод, заснований на загальному підході. Також на основі загального підходу розроблено методи виявлення таких порушень цілісності як масштабування та розмиття, що на даний момент є дуже ефективними, проте також вони мають певні недоліки.

У зв'язку з цим можна констатувати, що задача детектування порушення цілісності цифрового зображення не є до кінця вирішеною. Таким чином, тема кваліфікаційної роботи бакалавра «Розробка програмного забезпечення для комплексної перевірки цифрових зображень на наявність порушень їх цілісності» є важливою та актуальною.

Мета даної роботи – підвищення ефективності виявлення масштабування як порушення цілісності цифрового зображення.

Для досягнення даної мети необхідно вирішити наступні задачі.

1. Огляд сучасних методів виявлення порушення цілісності цифрового зображення.

2. Вибір та обґрунтування алгоритму виявлення масштабування для його модифікації.

3. Аналіз алгоритму на предмет його вдосконалення.

4. Модифікація алгоритму.

Об'єкт дослідження – процеси детектування несанкціонованої зміни цифрового зображення.

Предмет дослідження – алгоритм виявлення порушення цілісності цифрового зображення.

Практичне значення одержаних результатів. Практична цінність роботи полягає у модифікації алгоритму виявлення масштабування та його реалізації, що може бути використано як складова систем захисту інформації, інформаційних систем різного наповнення будь-якого закладу, підприємства, тощо. Отримані в роботі результати опубліковано у фаховому науковому виданні Інформатика та математичні методи в моделюванні [1].

1 ОГЛЯД СУЧАСНИХ МЕТОДІВ ВИЯВЛЕННЯ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

1.1 Підходи та методи вирішення проблеми виявлення порушень цілісності цифрового зображення

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

Соціальні мережі та їх тотальна популярність, розвиток IT-технологій, здешевлення та загальнодоступність графічних редакторів, таких як, наприклад, Adobe Photoshop або GIMP, призводить до росту комп’ютерної злочинності, зокрема, до значного збільшення випадків несанкціонованих змін ЦЗ.

Мільйони доларів виділяють щорік на боротьбу з комп'ютерною злочинністю розвинені країни світу. Важко виділити сфери нашого життя (медицина, охоронні системи, системи безпеки, судові розгляди), де б не використовувались цифрові зображення, аудіо- та відео-сигнали. Найчастіше фальсифікації піддається графічна інформація (цифрові зображення, цифрове відео). Зважаючи на це особливо актуальним на сьогоднішній день є уміння відрізнити підробку від справжнього сигналу.

Цифрове відео представляє собою послідовність кадрів, тобто аналіз цифрового відео на наявність фальсифікації може бути зведений до аналізу окремих кадрів відео послідовності (цифрових зображень). Тому для

простоти викладання далі мова йтиме про цифрові зображення, але усі отримані результати можуть бути використані і для цифрових відео-послідовностей також.

Так як існує безліч способів зміни стану цифрового зображення, 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.

Усі 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 інформації за способом їх реалізації поділяють на програмні, криптографічні, технічні та організаційні.

Методи пасивного захисту інформації в свою чергу поділяють за способом їх реалізації на методи експертної оцінки, програмно-технічні та програмні.

Програмно-технічні методи пасивного захисту інформації ґрунтуються 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 цифрових зображень 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 цифрових зображень від несанкціонованих змін заснований на аналізі вбудованого в об'єкт, що захищається, цифрового водяного знаку (ЦВЗ) [5-10]. Розробки в цій галузі ведуть найбільші фірми 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 методами активного захисту інформації) та аналізу цифрових водяних знаків (здійснюваного методами пасивного захисту інформації) виконує стегосистема.

У більшості стегосистем для впровадження та виділення цифрових водяних знаків використовується ключ. Ключ може бути призначений для вузького кола осіб або ж бути загальнодоступним. Якщо цифрові водяні знаки використовується для підтвердження автентичності, то неприпустимі зміни контейнера повинні призводити до руйнування ЦВЗ, що і буде зафіксовано методами пасивного захисту інформації при його аналізі. Але метод з використанням ЦВЗ не позбавлений серйозних недоліків. У порушника на законних підставах може матися декодер – пристрій виявлення цифрових водяних знаків (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 не має.

Широке поширення сьогодні набули методи, засновані на аналізі EXIF-даних – додаткової інформації, що додається в медіафайли цифровою технікою безпосередньо при їх створенні [11]. 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 редагуванні файлу, але не визначають область і характер редагування, що не дає можливості використання їх для достовірного дослідження ЦЗ на предмет 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 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, розмиття).

Порушення цілісності у даній роботі визначимо як несанкціоновану зміну цифрового зображення. Під фальсифікацією (фотомонтажем) будемо розуміти заміну частини (частин) одного цифрового зображення частиною (частинами) іншого (цього ж) цифрового зображення.

З практики відомо, що при підробці фотографій дуже часто виникає необхідність дублювання яких-небудь об'єктів (додати людей в натовпі, вставити додаткове вікно в стіні будинку, змінити номерний знак і тому подібне) або приховування різних деталей (прибрати людину, дерево, літак і тому подібне). У одному з найуживаніших графічних редакторів на сьогоднішній день – Adobe Photoshop – для вирішення цього завдання найчастіше застосовують інструмент «Штамп». Цей інструмент використовується для переміщення клону об'єкту з однієї частини зображення в іншу шляхом паралельного перенесення, як правило, в межах однієї і тієї ж фотографії. Найзручніше «перекривати» об'єкт невеликими фрагментами, які доцільно брати з того ж ЦЗ поблизу оброблюваного об'єкту, аби мінімізувати відмінності світла/тіні, яскравості/контрастності. Дублювання об'єкту з тих же міркувань доцільно проводити, використовуючи одну і ту ж фотографію. У обох випадках відбувається копіювання (паралельне перенесення) груп пікселів з однієї частини ЦЗ в

іншу. Завдання полягає в тому, аби виявити групи пікселів ЦЗ, що повторюються. Якщо такі знайдуться, це свідчитиме про вживання «Штампу» в даній області.

В [20-21] розроблено методи пошуку клонованих ділянок, що використовують алгоритми SIFT і SURF (зіставлення частин зображень по ключових точках), які є одними з найбільш ефективних і швидких сучасних алгоритмів. Крім того, реалізації SIFT і SURF є в багатьох математичних бібліотеках. Ці методи є інваріантними до таких геометричних перетворень клонованих ділянок як поворот, масштабування, спотворення перспективи, зміна яскравості пікселів [22]. Однак, незважаючи на те, що дані алгоритми використовуються для пошуку об'єктів на зображенні, вони самі працюють не з об'єктами, SIFT і SURF ніяк не виділяють об'єкт з фону. Вони розглядають зображення як єдине ціле і шукають особливі точки цього зображення в областях високої контрастності [23]. Метод, заснований на цих алгоритмах, погано працює для об'єктів простої форми і без яскраво вираженої текстури. Також дані методи не придатні для виявлення клонованих ділянок малого розміру. Таким чином, їх використання для виявлення фотомонтажу потребує серйозного доопрацювання.

В [24] отримано критерій прояву ефекту подвійного квантування на гістограмах коефіцієнтів дискретного косинусного перетворення для цифрового сигналу; отримані і обґрунтовані особливості прояву ефекту подвійного квантування в реальних умовах функціонування системи – за наявності шумів округлення значень цифрового сигналу і шумів, що виникають в процесі друку і сканування цифрового зображення; отриманий кількісний параметр, що дозволяє відокремити негативний внесок області порушення цілісності від негативного впливу природних шумів в прояв ефекту подвійного квантування. В результаті даних досліджень автором розроблений метод перевірки цілісності цифрових сигналів, заснований на прояві ефекту подвійного квантування. Метод ефективно працює в реальних умовах функціонування системи, тобто при наявності шумів округлення,

сканування і друку, дозволяє проводити перевірку цілісності цифрових сигналів. Також розроблено метод уточнення локалізації області порушення цілісності ЦС, заснований на віртуальному збільшенні внеску області порушення цілісності в цифровий сигнал. Метод дозволяє локалізувати область фальсифікації, розміри якої можна порівняти з розмірами блоків при стандартному розбитті сигналу. При всіх перевагах даний метод не позбавлений недоліків: у разі використання для фотомонтажу ЦЗ в форматі без втрат його застосування стає неможливим.

Як відомо з відкритих джерел, популярним та успішним методом виявлення такої фальсифікації є метод, заснований на кореляції коефіцієнтів дискретного косинусного перетворення матриці зображення [20], проте, даний метод в реальних умовах вимагає значних обчислювальних витрат.

Активно протягом останнього десятиріччя розвиваються методи виявлення порушень цілісності цифрових зображень [26-34], засновані на Загальному підході до аналізу стану та технології функціонування інформаційної системи, який у свою чергу базується на матричному аналізі та теорії збурень. Головні положення загального підходу у контексті ЦЗ коротко описані далі.

В якості математичної моделі цифрового зображення можна використовувати його матрицю (скінчену множину матриць) яскравості пікселів. 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 отримуються за допомогою нормального сингулярного розкладання матриці (SVD) [26], то при вибраному матричному способі формалізації 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) [29], звідки випливає, що будь-яке перетворення ЦЗ формально представляється у вигляді сукупності збурень СНЧ і СНВ відповідної йому матриці (матриць).

На даний момент найефективнішим з точки зору точності локалізації клонованої ділянки є метод виявлення клонування, заснований на аналізі СНЧ блоків матриці ЦЗ. Основні кроки даного методу полягають у наступному. Матриця ЦЗ розбивається на пересічні блоки 8×8 так, щоб будь-які сусідні блоки відрізнялися на один стовбець або рядок. Для кожного блоку слід знайти множину сингулярних чисел. Наступним кроком є відкидання чотирьох найменших СНЧ у кожному блоці, залишивши найбільші. Порівняти попарно між собою усі блоки. Клонованими вважаються ті блоки, СНЧ в яких виявилися однаковими.

Проте, як виявилося при проведенні обчислювального експерименту при виконанні даної роботи, зовсім не обов’язково аналізувати усі зазначені вище сингулярні числа, що буде детально показано та обґрунтовано нижче.

Для експерименту базу цифрових зображень було утворено з ЦЗ форматів як з втратами (JPEG), так і без втрат (BMP). Цифрові зображення 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 розглядаються через погану якість, яка сама по собі викликає підозри щодо автентичності ЦЗ.

1.2 Загальний підхід до аналізу стану і технології функціонування інформаційної системи

Дуже активно розвиваються методи для виявлення порушень цілісності цифрових зображень [23-27]. Вони засновані на загальному підході до аналізу

стану та технології функціонування інформаційної системи (ЗПАІС), який у свою чергу базується на матричному аналізі та теорії збурень.

Відповідно до ЗПАІС будь-яка інформаційна система (ІС) може бути представлена у вигляді певної множини матриць кінцевої розмірності з дійсними елементами. У зв'язку з цим, аналіз будь-якої ІС можна звести до аналізу відповідних матриць [31].

Будь-яка ІС при обраному матричному способі формалізації може бути однозначно визначена сингулярним спектром (спектрами) і набором (наборами) сингулярних векторів (СНВ) відповідної їй матриці (матриць), тобто інформацію про стан будь-якої ІС несуть у собі сингулярні числа (СНЧ) і СНВ [32-33].

Нехай F – матриця, що визначає ІС. Згідно до ЗПАІС будь-яке перетворення ІС можна представити у вигляді збурення ΔF матриці F [31]

$$\bar{F} = F + \Delta F, \tag{1.1}$$

де $\bar{F}$ – матриця ІС після перетворення.

Так як довільна матриця однозначно визначається своїм сингулярним спектром, тобто множиною СНЧ та набором СНВ спеціального виду, що можуть бути отримані в результаті нормального сингулярного розкладання матриці (SVD) [26], тоді усі перетворення будь-якої ІС представляються у вигляді сукупності збурень СНЧ і СНВ її матриці, що випливає з (1.1).

Отже, аналіз перетворення ІС зводиться до аналізу характерних особливостей збурень СНЧ і СНВ відповідної матриці (матриць). СНЧ та СНВ несуть в собі всю інформацію про стан ЦЗ.

СНЧ нечутливі до збурюючих дій або добре зумовлені відповідно з формулою

$$\max_j \left|\sigma_j(F) - \sigma_j(F + \Delta F)\right| \le \|\Delta F\|_2 , \tag{1.2}$$

де $\sigma_j(F),\ \sigma_j(F+\Delta F)$ – СНЧ матриць F та $F+\Delta F$ відповідно;

$\|\Delta F\|_2$ – спектральна норма ΔF.

Виходячи з нерівності (1.2) можна помітити, що збурення СНЧ співвіднесені з величиною збурюючої дії [32].

Також відповідно до [32] відокремленістю СНЧ σ_i є

$$svdgap(i,F) = \min_{i \neq j} \left|\sigma_j - \sigma_i\right|. \quad (1.3)$$

Виходячи з (1.3) можна отримати

$$\frac{1}{2}\sin 2\theta_i \leq \frac{\|\Delta F\|_2}{svdgap(i,F)},$$

де θ_i – кут між відповідними вихідним та обуреним ортонормованими СНВ u_i та $\overline{u_i}$ і матриць F та $F+\Delta F$, відповідно.

Відокремленість СНЧ є мірою чутливості відповідного СНВ до збурюючих дій. СНВ, що відповідають СНЧ з малою відокремленістю, чутливі до малих збурень. Протилежна ситуація із СНВ, що відповідають СНЧ з великою відокремленістю, адже вони не чутливі до малих збурень [30].

Цифрові зображення, можна розглядати у якості ІС. Порушення цілісності ЦЗ відповідно до ЗПАІС формально може бути представлене у вигляді збурення (сукупності збурень СНЧ і СНВ) вихідної матриці (множини матриць) ЦЗ [29, 33].

Збурення аналізованих параметрів ЦЗ несуть в собі інформацію про силу впливу збурюючої дії. Реакція СНВ матриці ЦЗ на збурення різна, а для деяких СНВ (що відповідають СНЧ з малою відокремленістю) – непередбачувана [33, 34]. Навіть невеликий вплив на ЦЗ, як шум, що може виникнути при скануванні, можливо, призведе до значних збурень СНВ його матриці (матриць). Тому в загальному випадку величину збурюючої дії не можна співвіднести з величиною збурення СНВ, з чого випливає

недоцільність використання СНВ для аналізу ЦЗ на наявність фальсифікації. Збурення ж СНЧ завдяки їх добрій обумовленості, що випливає з (1.2), можна порівняти з величиною збурюючої дії, що характеризує її силу.

Таким чином, в якості набору формальних параметрів, що характеризують цифрове зображення, аналіз яких доцільно використовувати для виявлення порушення його цілісності, обрано набір СНЧ [34].

1.3 Вплив клонування на матрицю цифрового зображення

При фальсифікації ЦЗ засобами графічних редакторів дуже часто застосовується інструмент «штамп» (клон). Оскільки штамп – ні що інше, як клонування пікселів, абсолютно природно для повторюваних блоків мати однакові СНЧ за умови, що ЦЗ не піддавалося квантуванню після фальсифікації, тобто зберігалося у форматі без втрат. Розглянемо детально обчислювальний експеримент, проведений у [36]. На прикладі ЦЗ розміром 16×16 пікселів, розбитого на непересічні блоки 8×8 пікселів, виконане дублювання (клонування) верхнього лівого блоку в сусідній блок (вправо). Для кожного блоку визначено множину сингулярних чисел.

Проведений експеримент показав: повторювані блоки мають абсолютно однакові СНЧ, як і очікувалося у зв'язку з однозначністю сингулярного спектру матриці. Тому для пошуку заміщуючої області (клону) має сенс порівнювати СНЧ блоків і виділяти, як клоновані, ті блоки, сингулярні числа яких рівні [36].

У даному експерименті блок-прототип було продубльовано чітко у сусідній блок, тобто стандартне розбиття на блоки 8×8 пікселів і лінійна залежність між пікселями при обчисленні СНЧ не порушені. Але в реальних умовах така ситуація малоймовірна. Необхідно вибрати таке розбиття на блоки, яке дало б можливість адекватно провести дослідження на наявність клонування.

Нехай є зображення, яке піддається обробці інструментом «штамп» в графічному редакторі. Тоді для ефективного виявлення клонування у вказаний вище спосіб рекомендується розбивати матрицю ЦЗ на блоки, що

відрізняються від сусідніх на один стовбець або рядок.

Тепер детально розглянемо СНЧ блоків, які є клонами. Як ми можемо бачити, вони є однаковими. У ЗПАІС встановлено відповідність між сингулярним та частотним спектрами ЦЗ, згідно до якої найбільші СНЧ відповідають низькочастотній складовій сигналу ЦЗ. Із зменшенням СНЧ вклад низьких частот стає меншим, а вклад високих частот збільшується. Це свідчить про те, що найбільше СНЧ відповідає головним чином фоновій складовій блоку матриці ЦЗ, а найменші СНЧ – контурній. Через особливості людського зору основну візуальну інформацію людина отримує саме з низьких частот сигналу зображення, за які відповідає головним чином найбільше СНЧ. Тож з метою зменшення обчислювальних витрат методу виявлення клонування є сенс порівнювати не усі СНЧ блоків, а лише найбільше. Обчислювальна складність методу при такій модифікації зменшиться на порядок, а ефективність не знизиться, що буде доведено у наступному розділі при проведенні обчислювального експерименту.

1.4 Вплив деяких видів обробки на матрицю цифрового зображення

Фотографії відображають лише одну мить в часовому просторі. Та все ж таки рух можна передати на фотографії як різними фотографічними прийомами, так і за допомогою деяких дій в графічному редакторі, наприклад, за допомогою розмиття. У графічних редакторах запропоновано багато видів розмиття з різними параметрами, які можуть бути використані при постобробці фальсифікованого ЦЗ. Візуальний ефект розмиття ЦЗ можна побачити на рисунку 1.1.

Розмиття часто використовується в фотоіндустрії з некримінальною метою. Це може бути надання бажаного ефекту як зображенню в цілому, так і його частини, наприклад, для акцентування уваги на деякий об'єкт за допомогою зменшення глибини різкості зображуваного простору. Такий ефект можливий при макрозйомці, де об’єкт чіткий, а решта зображення розмита, а також при зйомці об'єкта із проводкою. Глибиною різкості

зображуваного простору (ГРЗП) називається діапазон відстаней на фотографії, в якому об'єкти зйомки сприймаються різкими.

а) б)

Рисунок 1.3 – Вихідне ЦЗ (а); розмите ЦЗ (б)

Цей діапазон відстаней також називають зоною різкості та вона знаходиться навколо точки фокусування.

Якщо об’єкти зйомки відображаються різкими на малому діапазоні відстаней навколо точки фокусування, то вважають, що такий знімок зроблено з малою глибиною різкості. 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). Саме такі зображення отримуються при макрозйомці та відтворенні ефекту руху за допомогою фотографічного прийому «Проводка». Якщо можливо розрізнити чіткі деталі у будь-якій області зображення чи хоча б на більшій частині зображення, то це означає, що знімок зроблено з великою глибиною різкості: об'єкти в кадрі виглядають різкими і не розмитими на великому діапазоні.

У [24] показано порівняльний аналіз методів виявлення розмиття та зроблено висновок, що метод, заснований на ЗПАІС, є найефективнішим сьогодні [24-26], адже головною його перевагою є здатність відокремлювати ЦЗ, що розмиті програмними засобами, від тих, що було зроблено із малою глибиною різкості зображуваного простору.

Розмиття впливає на сингулярні числа зображення, зменшуючи

швидкість їх росту настільки, що за цим зменшенням можна судити, чи зображення оброблене фільтром розмиття, чи ні.

1.5 Вплив масштабування на матрицю цифрового зображення

Масштабування також вдало вдається виявляти за допомогою загального підходу, на основі якого розроблено метод виявлення масштабування. Цей метод засновано на аналізі матриці нульових сингулярних чисел блоків матриці цифрового зображення. При масштабуванні з’являється лінійна залежність між рядками та/або стовпцями матриці цифрового зображення. Сингулярні числа реагують на лінійну залежність рядків та стовпців своїм обнулінням. Таким чином в області, що відповідає масштабованій ділянці цифрового зображення, з’являться нульові сингулярні числа в блоках матриці зображення, детектування чого і дозволяє виявляти наявність масштабування.

Для аналізу зображення на предмет наявності масштабування зображенню необхідно поставити у відповідність матрицю нульових сингулярних чисел блоків, кожний елемент якої відповідає одному блоку ЦЗ та дорівнює кількості нульових сингулярних чисел в ньому. Масштабованими будуть ті частини, яким відповідають блоки з великою кількістю нульових сингулярних чисел. Даний метод ефективний, проте має велику кількість хибних тривог.

Виходячи з проведеного аналізу можна зробити наступні висновки: задача доказу або виявлення порушення цілісності цифрових зображень не вирішена до кінця. Особливістю проведення несанкціонованих змін цифрових зображень у даний момент є практично обов'язкове використання таких програмних засобів, що не може не враховуватися при розробці методів і алгоритмів виявлення порушень цілісності ЦЗ. Виявленню результатів обробки фальсифікованих цифрових зображень засобами графічних редакторів приділено недостатньо уваги. При виявленні обробки експертними методами в одержуваний результат вноситься суб'єктивна складова.

Найефективнішими у даний час методами виявлення порушень цілісності ЦЗ є методи, засновані на загальному підході до аналізу стану і технології функціонування інформаційної системи. Тому у даній роботі доцільно використовувати результати досліджень, отриманих раніше при розробці зазначених методів, для досягнення поставленої у роботі мети.

Таким чином, у першому розділі вирішені задачі один та два з переліку завдань, поставлених у кваліфікаційній роботі.

2 АЛГОРИТМИ КОМПЛЕКСНОЇ ПЕРЕВІРКИ ЦИФРОВОГО ЗОБРАЖЕННЯ

2.1 Контекстне масштабування як порушення цілісності цифрового зображення

При дублюванні об'єкта, як і при його приховуванні, відбувається копіювання груп пікселів з однієї частини зображення в іншу шляхом їх паралельного перенесення. Дана операція (клонування) часто проводиться за допомогою інструменту, реалізованого в більшості графічних редакторів, званого Штамп (Клон). Однак виконання цієї операції можливе і без застосування даного інструменту. Це можна виконати звичайним виділенням групи пікселів та копіюванням їх в іншу частину цього ж зображення. Якщо клонування виконували таким чином, то клоновану ділянку також можна масштабувати та підганяти за розміром до контексту цифрового зображення.

У розробленому в [36] методі порівнюються суми СНЧ у блоках (для клонованих блоків ці суми будуть рівні). Основні кроки алгоритму виявлення клонування, заснованого на аналізі сингулярних чисел блоків його матриці, представлені нижче.

1. Розбити матрицю F ЦЗ на 8×8-блоки $F_{ij}, i=1,2\ldots,(n-7),\ j=1,2\ldots,(m-7)$, що перетинаються так, аби кожний блок відрізнявся від сусіднього на один рядок (стовпець).

2. Побудувати матрицю S з елементами $s_{ij}=\sum_{k=1}^{4}\sigma_k$, $i=1,2\ldots,(n-7)$, $j=1,2\ldots,(m-7)$, де $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ – найбільші СНЧ відповідного блоку $F_{ij}, i=1,2\ldots,(n-7),\ j=1,2\ldots,(m-7)$.

3. Побудувати матрицю клонування (МК) C з елементами c_{ij}, $i=1,2\ldots,(n-7)$, $j=1,2\ldots,(m-7)$; c_{ij} відповідає блоку F_{ij} ЦЗ. Для визначення c_{ij} порівняти s_{ij} попарно з усіма елементами матриці S :

Якщо для s_{ij} знайдеться такий елемент $s_{kl}, k \neq i, l \neq j$ матриці S , для якого виконується нерівність $\left|s_{ij} - s_{kl}\right| < \delta$

тоді $c_{ij} = 1$,

інакше $c_{ij} = 0$.

4. Елементи $c_{ij} = 1$ матриці C відповідають клонованим блокам ЦЗ.

Однак даний алгоритм буде дієздатним лише при виконанні клонування без застосування масштабування до клонованої ділянки у випадку, коли оброблене зображення збережено у форматі без втрат.

Вплив деяких видів фільтрів графічних редакторів на виявлення масштабованих клонованих ділянок також робить неможливим застосування методу виявлення клонування. Як відомо, розмиття призводить до зменшення високочастотної складової сигналу. Із [24] відомо, що при застосуванні розмиття СНЧ мають тенденцію зменшуватися наступним чином: СНЧ, які відповідають високим частотам ЦЗ, тобто найменші, а також середні за значенням СНЧ будуть змінені найбільше – швидкість їхнього зросту буде близька до нуля, на відміну від швидкості росту найменших СНЧ нерозмитого зображення. Проте виявлення розмиття у даному випадку вже вказуватиме на наявність порушення цілісності цифрового зображення. Для цього можна використати метод, алгоритм якого наведемо далі.

Нехай F – $n \times m$-матриця ЦЗ.

1. Розбити матрицю F стандартним чином на 8×8-блоки $F_{ij}, i = 1,2\ldots, [n/8], j = 1,2\ldots, [m/8]$.

2. Побудувати МШР W з елементами w_{ij}, $i = 1,2\ldots, [n/8], j = 1,2\ldots, [m/8]$, при цьому для визначення елементів w_{ij}:

2.1 Для блоку F_{ij} знайти сингулярний розклад: $F_{ij} = U_{ij}\Sigma_{ij}V_{ij}^T$, де U_{ij}, V_{ij} - ортогональні 8×8 – матриці лівих та правих СНВ F_{ij} відповідно, $\Sigma_{ij} = diag(\sigma_1,...,\sigma_8)$ - матриця СНЧ, $\sigma_1 \geq ... \geq \sigma_8 \geq 0$.

2.2 Для $\sigma_l, l = 4,...,8$ блоку F_{ij} побудувати лінійну апроксимуючу функцію $y = ax + b$.

2.3 $w_{ij} = a$.

3 *Якщо* $VMV_c > 1{,}75$

то зображення не розмите, *інакше* зображення розмите.

Використовуючи властивості сингулярних чисел блоків матриці можна також детектувати масштабування не клонованих ділянок, а тих, що було взято з інших цифрових зображень.

2.2 Виявлення масштабування

Один з найпопулярніших методів редагування цифрових зображень, що його використовують при підробці світлин – масштабування, контекстно-залежне або загальне. Контекстно-залежне масштабування – це заміна частини основного зображення частиною цього ж або іншого зображення з подальшим збільшенням або зменшенням.

Один з найефективніших сучасних методів виявлення масштабування, заснований на аналізі матриці нульових сингулярних чисел блоків (МНСЧБ) цифрового зображення. Встановлено, що кількість нульових сингулярних чисел блоків вказує на лінійну залежність рядків та стовпців матриці. Лінійна залежність обов'язково виникає при масштабуванні та сигналізує про можливе порушення цілісності цифрового сигналу. Але лінійна залежність рядків та стовпців матриці також характерна зображенню, збереженому у форматі з втратами. Експериментально встановлено, що елементи МНСЧБ останнього і першого рядка, останнього і першого стовпця масштабованої ділянки завжди приймають значення більші, ніж елементи в середині масштабованої частини, утворюючи прикордонний контур. Елементи масштабованої частини виділяються на загальному фоні при допущені того, що блоки немасштабованих частин зображення не містять нульових сингулярних чисел.

Розглянемо приклад впливу масштабування на матрицю зображення в

умовах збереження в форматі з втратами (рис.2.1).

$$R_1=\begin{pmatrix}177 & 175 & 178\\ 181 & 182 & 184\\ 180 & 183 & 186\end{pmatrix} \quad R_2=\begin{pmatrix}176 & 175 & 175 & 170 & 170 & 170\\ 176 & 175 & 173 & 173 & 171 & 172\\ 180 & 180 & 179 & 180 & 179 & 179\\ 180 & 181 & 180 & 181 & 180 & 180\\ 179 & 180 & 180 & 180 & 180 & 179\\ 181 & 182 & 183 & 181 & 180 & 181\end{pmatrix}$$

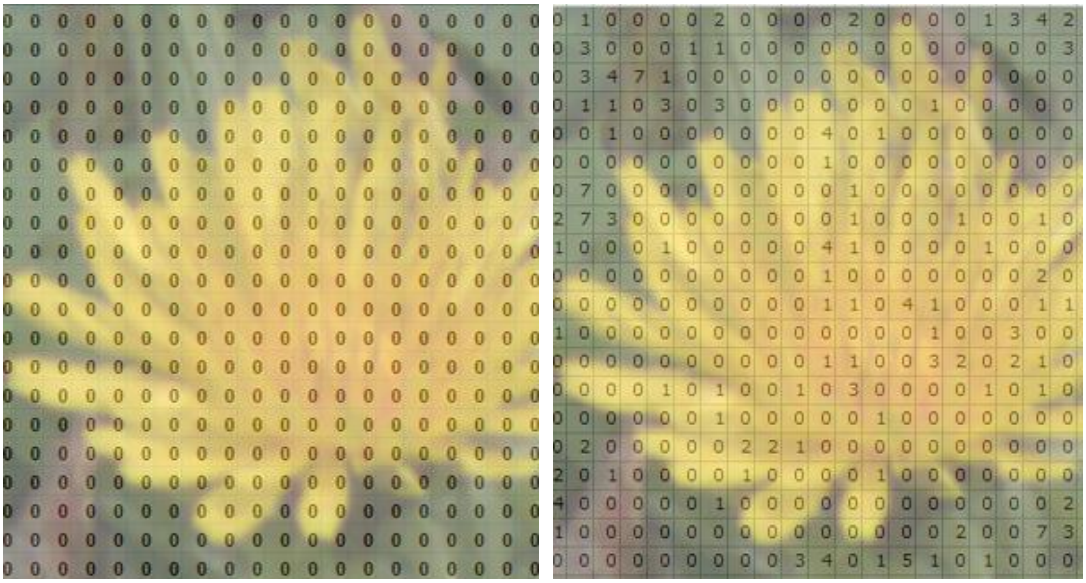
Рисунок 2.1 – Підматриці зображення:
R_1 – оригінальне зображення розміром 3×3, R_2 – масштабоване зображення розміром 6×6

На рисунку 2.1 можемо бачити фрагмент червоної компоненти в колірній моделі RGB зображення розміром 3×3 та масштабоване вдвічі зображення, яке було збережено в форматі з втратами. Після масштабування та збереження ЦЗ в форматі з втратами з'являються значення, близькі або рівні значенням, що їх оточують. Це і пояснює виникнення нульових сингулярних чисел блоків матриці цифрового зображення. На рисунку 2.2 можемо бачити приклад масштабування на цифровому зображенні.

а) б)

Рисунок 2.2 – Приклад масштабування: а) оригінальне зображення, б) фальсифіковане зображення

Розглянемо приклад МНСЧБ для оригінального зображення та зображення, яке було збільшено (рис. 2.3).



а) б)

Рисунок 2.3 – МНСЧБ зображення до масштабування (а), після масштабування (б)

При збільшенні зображення на МНСЧБ з’являються значення від 1 до 7, це і вказує нам на наявність даного виду порушення цілісності цифрового зображення.

Алгоритм методу виявлення масштабування, заснований на аналізі нульових сингулярних чисел блоків його матриці, складається з наступних кроків.

1. Розбити матрицю F стандартним чином на 8×8-блоки $F_{ij}, i=1,2\ldots,[n/8],\ j=1,2\ldots,[m/8]$.

2. Побудувати МНСЧБ $M([n/8],[m/8])$ з елементами m_{ij}, $i=1,2\ldots,[n/8],\ j=1,2\ldots,[m/8]$, де значення m_{ij} визначає кількість нульових сингулярних чисел блоку $F_{ij}, i=1,2\ldots,[n/8],\ j=1,2\ldots,[m/8]$.

3. Матрицю M розбити на підобласті $M_l, l=1,2\ldots t$.

4. Виділити серед M_l підобласті, які містять елементи $m_l \geq 1$. Дані під області відповідають масштабованим частинам.

На рисунку 2.4 розглянемо приклад роботи алгоритму для зображення, в якому попередньо було продубльовано його ж частину та масштабовано її.

Такий фотомонтаж було збережено у форматі без втрат.

Рисунок 2.4 – Тестове цифрове зображення

Рисунок 2.5 – Бінарне зображення МНСЧБ тестового зображення

Матриця нульових сингулярних чисел представлена у вигляді бінарного зображення, де 0 позначено чорним кольором, а не 0 – білим. Тобто білі частини відповідають масштабуванню. Проте, білим також позначено помилки другого роду. Спробуємо їх зменшити. Поекспериментуємо з пороговим значенням для елементів МНСЧБ. Будемо

виділяти чорним елементи, менші за двійку (рис. 2.6, а), трійку (рис. 2.6, б) та четвірку (рис. 2.6, в).

а) б) в)

Рисунок 2.6 – Бінарне зображення МНСЧБ: а) обнуління одиниць; б) обнуління одиниць і двійок; в) обнуління одиниць, двійок та трійок

Отже, якщо ставити за мету збереження точності локалізації масштабованої частини зображення, то в якості порогу для обнуління слід обрати значення 3.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ПРОДУКТУ

3.1 Обґрунтування вибору програмного середовища

Описані в другому розділі алгоритми реалізовано в програмному середовищі MATLAB R2010a. Сучасна комп'ютерна математика пропонує цілий набір інтегрованих програмних систем і пакетів програм для автоматизації математичних розрахунків. MATLAB – одна з найстаріших, ретельно опрацьованих і апробованих часом систем автоматизації математичних розрахунків, побудована на розширеному поданні та застосуванні матричних операцій. Це знайшло відображення у назві системи (MATrix LABoratory – матрична лабораторія). Однак синтаксис мови програмування системи продуманий настільки ретельно, що ця орієнтація зовсім не відчувається користувачами, яких безпосередньо матричні обчислення не цікавлять. Матриці широко застосовуються в складних

математичних розрахунках, наприклад, при вирішенні задач лінійної алгебри та математичного моделювання статичних і динамічних систем і об'єктів. Вони є основою автоматичного завдання і рішення рівнянь стану динамічних об'єктів і систем. Прикладом може служити розширення MATLAB – Simulink. Це істотно підвищує інтерес до системи MATLAB, що увібрала в себе кращі досягнення в галузі швидкого вирішення матричних задач.

Проте, в даний час MATLAB далеко вийшла за межі спеціалізованої матричної системи і стала однією з найбільш потужних універсальних та інтегрованих систем. Слово «інтегровані» вказує на те, що в цій системі об'єднані зручна оболонка, редактор виразів і текстових коментарів, обчислювач та графічний програмний процесор. У новій версії використовуються такі потужні типи даних, як багатовимірні масиви, масиви осередків і розріджені матриці, що відкриває можливості застосування системи при створенні та налагодженні нових алгоритмів матричних та заснованих на них паралельних обчислень і великих баз даних.

В цілому MATLAB – це унікальна колекція реалізацій сучасних чисельних методів для комп'ютерів, створених за останні три десятки років. Вона увібрала в себе досвід, правила і методи математичних обчислень, накопичені за тисячі років розвитку математики. Це поєднується з потужними засобами графічної візуалізації і навіть анімаційної графіки. Графічний інтерфейс користувача (GUI): GUI-Guide – інтерактивний засіб побудови графічного інтерфейсу користувача; редактор властивостей графічних об'єктів; панелі списків, включаючи списки з великим вибором; форма діалогових панелей і панелей повідомлень; підготовка документів у форматі HTML. Математичні обчислення та аналіз даних: обчислення власних значень і сингулярних чисел для матриць розрідженої структури; двовимірні квадратурні формули; багатовимірна інтерполяція.

Переваги MATLAB:

- інструменти, що дозволяють за допомогою миші інтерактивно редагувати і анотувати графіки, оптимізація коду і пам'яті графічних команд і

атрибутів;

- для прискорення матричних обчислень поліпшені алгоритми і використовується оптимізована бібліотека LAPACK; завдяки FFTW бібліотеці прискорені інтегральні перетворення; потужні і точні алгоритми інтегрування диференціальних рівнянь і квадратури;
- сучасні функції візуалізації: виведення на екран двомірних зображень, поверхонь і об'ємних фігур у вигляді прозорих об'єктів; інструментальна панель Camera для управління перспективою і прискорення виведення графіки;
- сучасні інструменти проектування графічного інтерфейсу користувача;
- додаток MATLAB для системи розробки Visual Studio, що дозволяє автоматично, безпосередньо з Microsoft Visual Studio, перетворювати C та C++ коди у виконувані MATLAB файли (MEX-файли);
- змінні в MATLAB чутливі до регістру в імені, не вимагають визначення типу змінної (ціла, речова, масив), для перегляду значення змінної достатньо набрати її ім'я в командному рядку (без крапки з комою в кінці), для знищення змінної треба використовувати команду clear.

Редактор GUIDE викликається командою guide з командного вікна або шляхом виконання ланцюжка команд головного меню File (Файл) → New (Новий) → GUI (графічний інтерфейс).

Також в MATLAB виділяється серед інших програмних середовищ тим, що в ньому є можливість користування влаштованими функціями, чого нема, наприклад, в C# та C++.

3.2 Реалізація алгоритмів виявлення масштабування цифрового зображення

Програмний продукт навмисне спроектовано максимально простим та інтуїтивно зрозумілим. Усі алгоритми реалізовано та розміщено так, щоб можна було бачити всі можливості програмного продукту. Розглянемо спочатку інтерфейс програмного продукту для проведення тестування.

Отже, перше, що необхідно виконати, це завантажити зображення, натиснувши кнопку «Завантажити зображення», яка знаходиться в лівій частині вікна (рис.3.1).

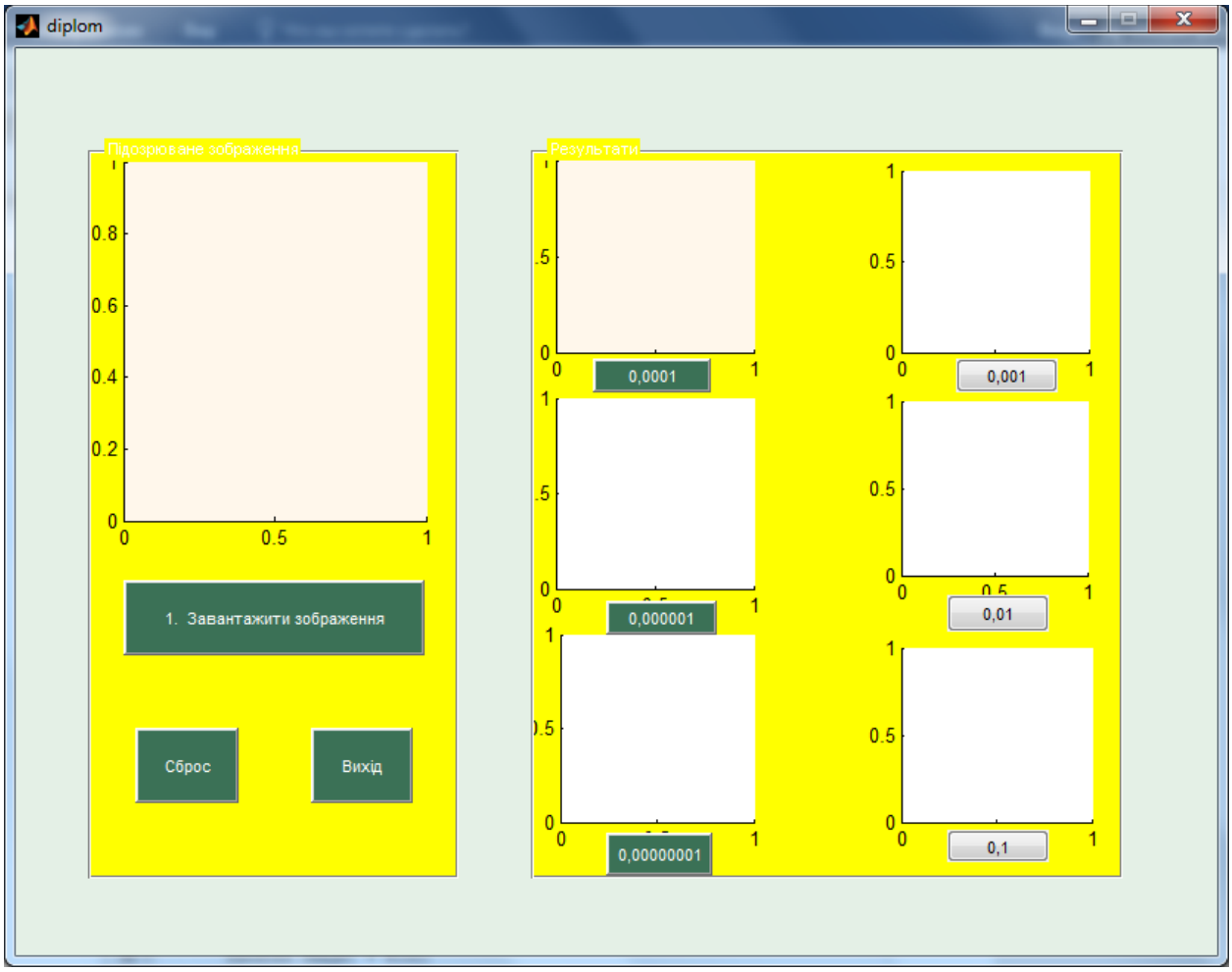


Рисунок 3.1 – Інтерфейс програмного продукту для проведення експериментів

Програмний код кнопки «Завантажити зображення» показано на рисунку 3.2.

```
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);
52      %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Рисунок 3.2 – Програмний код кнопки «Завантажити зображення»

Натиснувши на цю кнопку, побачимо контекстне меню вибору файлів на комп’ютері (рис.3.3).

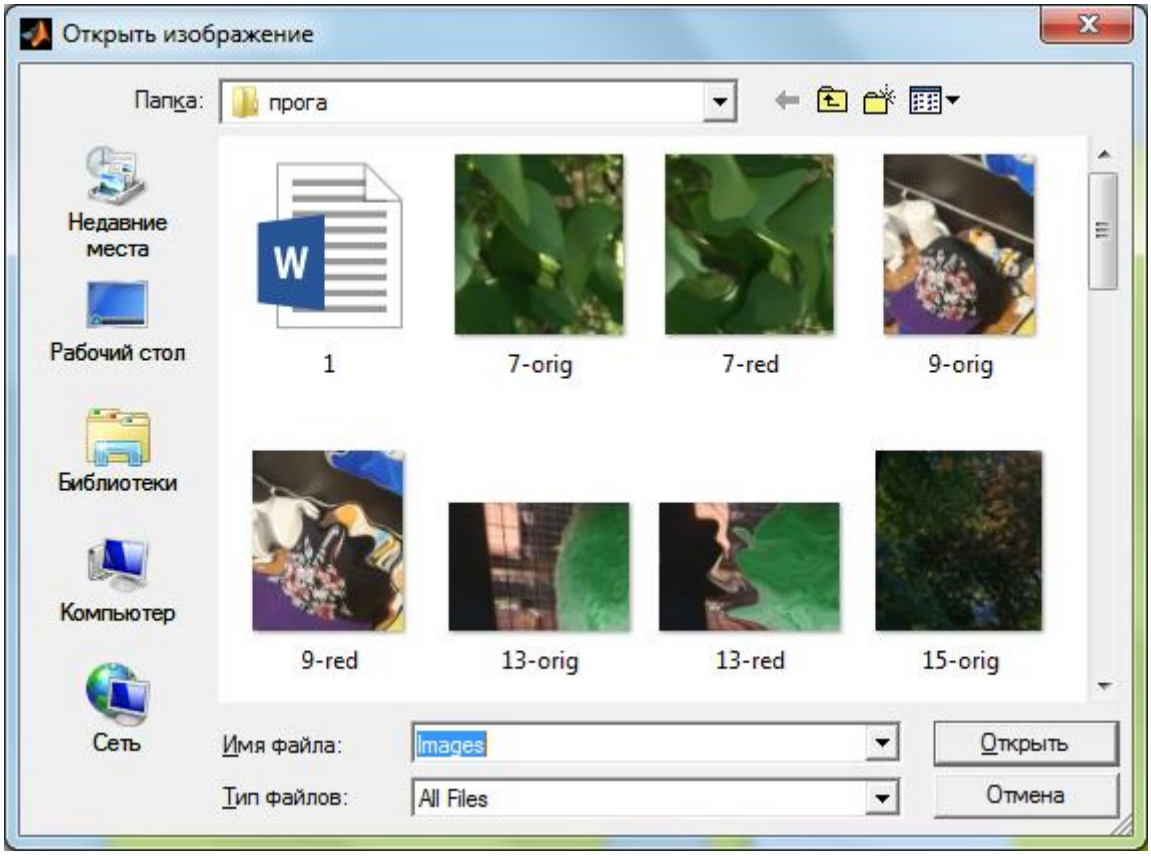


Рисунок 3.2 Вибір зображення для перевірки

Обираємо зображення, яке бажаємо перевірити. Зображення буде

завантажено у об’єкт над кнопкою «Завантажити зображення».

Після цього обираємо порогове значення, за яким буде сформовано матрицю нульових сингулярних чисел блоків. Можна обрати будь-яку. Ми натиснемо усі. Загальна процедура цих кнопок наведена на рисунку 3.3. Різниця буде у пороговому значенні.

```
176 -    T{1}=handles.Image1;
177 -    IZ=double(T{1});
178 -    IZ=IZ(:,:,1);
179 -    n=fix((size(IZ,1))/8)*8;
180 -    m=fix((size(IZ,2))/8)*8;
181 -    IZ=IZ(1:n,1:m);
182 -    svd_IZ = blkproc(IZ,[8 8],'svd(x)');
183 -    MNSVD = blkproc(svd_IZ,[8 1],'length(find(x<0.00000001))');
184 -    [h w]=size(MNSVD);
185 -    for i=1 : h
186 -        for j = 1:w
187 -            if MNSVD(i,j)<3
188 -                MNSVD(i,j)=0;
189 -            end
190 -        end
191 -    end
192 -    axes(handles.axes5);
193 -    imshow(MNSVD);
194
```

Рисунок 3.3 - Процедура «0,00000001»

Процедура для даного порогового значення, як бачимо, доволі проста. Елементи матриці нульових сингулярних чисел, що менші за трійку, прирівнюються до нуля. Це дозволяє зменшити кількість хибних тривог, не втративши при цьому точність локалізації масштабованої частини.

І зовсім прості процедури «СБРОС» та «ВИХІД», показані на рисунках 3.4 і 3.5 відповідно.

```
103      function pushbutton4_Callback(hObject, eventdata, handles)
104 -    axes(handles.axes1);
105 -    cla
106 -    axes(handles.axes2);
107 -    cla
108 -    axes(handles.axes4);
109 -    cla
110 -    axes(handles.axes5);
111 -    cla
112
```

Рисунок 3.4 - Процедура «СБРОС»

```
117      function pushbutton5_Callback(hObject, eventdata, handles)
118 -    selection = questdlg(['Выход ' get(handles.figure1,'Name') '?'],...
119                           ['Выход ' get(handles.figure1,'Name') '...'],...
120                           'Да','Нет','Да');
121 -    if strcmp(selection,'Нет')
122 -        return;
123 -    end
124 -    delete(handles.figure1)
```

Рисунок 3.5 - Процедура «ВИХІД»

Таким чином, в даному розділі вирішено задачу 4 з переліку задач, поставлених для досягнення мети кваліфікаційної роботи.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Забезпечення безпечних і здорових умов праці в значній мірі залежить від правильної оцінки небезпечних, шкідливих виробничих факторів. Однакові по складності зміни в організмі людини можуть бути викликані різними причинами. Це можуть бути фактори виробничого середовища, надмірне фізичне і розумове навантаження, нервово-емоційна напруга, а також різне сполучення цих причин.

У даному розділі вирішується питання охорони праці інженера програміста на стадії модифікації алгоритму виявлення масштабування для виявлення деяких порушень цілісності цифрового зображення. Ця робота виконується інженером-програмістом у офісному приміщенні. Тому як об’єкт дослідження з охорони праці, вибираємо робоче місце інженера-програміста.

Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів. Організація робочого місця інженера-програміста. Приміщення, в якому працює програміст, має загальну площу 44 м^2, висоту стелі 3,8 м. У приміщенні знаходиться 4 робочих місць з ПК. Кожне робоче місце обладнане робочим столом площею

1,2 м^2, стільцем та персональним комп'ютером, що складається з монітора, системного блоку, клавіатури та миші. Слід відзначити, що площа одного робочого місця оператора ПК не повинна бути меншою за 6 м^2, а об'єм не менший за 20 м^3, тобто площі та об'єму даного приміщення вистачає для розташування робочих місць інженерів-програмістів.

Робота користувача ПК виконується в одноманітній позі в умовах обмеження загальної м'язової активності при рухливості кистей рук, великому напруженні зорових функцій і нервово-емоційній напрузі під впливом наступних фізичних факторів:

– електростатичного поля;

– електромагнітних випромінювань у наднизькочастотному, низькочастотному та середньочастотному діапазонах (5 Гц – 400 кГц);

– рентгенівського, ультрафіолетового та інфрачервоного випромінювань;

– випромінювань видимого діапазону;

– акустичного шуму;

– незадовільного рівня освітленості;

– незадовільних метеорологічних умов.

Освітлення робочого місця інженера-програміста. Приміщення, обладнані ПК з ВДТ повинні мати природне і штучне освітлення, оскільки при недостатньому освітленні різко знижується продуктивність праці користувачів ПК, спостерігається швидка їх стомлюваність, а також можливе виникнення короткозорості.

Вимоги до природного та штучного освітлення приміщень, обладнаних ПК з ВДТ, визначаються згідно ДБН В.2.5-28-2018 «Природне і штучне освітлення». Природне освітлення має здійснюватися через світлові прорізи, орієнтовані переважно на північ або північний схід і забезпечувати коефіцієнт природної освітленості не нижче 1,5 %.

Значення освітленості на поверхнях робочих столів, в зоні розміщення документів, має становити 300 – 500 лк. Показник засліпленості для джерел

загального штучного освітлення в приміщеннях не повинен перевищувати 20, а показник дискомфорту – не більш 40.

Яскравість світлових поверхонь (вікна, джерела штучного освітлення тощо), розташованих в поле зору, не повинна перевищувати 200 кд/м^2. Яскравість відблисків на екрані дисплея не повинна перевищувати 40 кд/м^2, а яскравість стелі, при використанні системи відбитого освітлення, не повинна перевищувати 200 кд/м^2.

Коефіцієнт запасу для освітлювальних установок загального освітлення приймається рівним 1,4. Величина коефіцієнта пульсації освітленості не повинна перевищувати 5 %.

Причинами виникнення небезпечних і шкідливих факторів є:

– відсутність чи недостатність природного освітлення;

– недостатня освітленість робочої зони;

– прямий чи відбитий блиск.

Причини виникнення вищевказаних факторів:

– відсутність або недостатні розміри вікон;

– відсутність або недостатня кількість світильників;

– недоліки освітлення і неправильне розташування дисплея.

Найменший об’єкт розрізнення залежить від класу монітора. У нашому випадку використовується монітор SVGA з найменшим розміром об’єкта розрізнення 0,234 мм.

Найменшим об’єктом розрізнення на екрані монітора є крапка розміром 0,26 × 0,25 мм. Фон, з яким працює користувач, має чорний або білий, або синій колір, а колір символів коливається від білого до чорного, включаючи всі можливі кольори, однак вибір залежить від працівника. Контраст і чіткість зображення можна регулювати, не втручаючись в програму, для чого необхідно скористатися регулюванням на моніторі.

Виробничі випромінювання. Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітору комп’ютера представлені в табл. 4.2. Нормованим параметром

невикористаного рентгенівського випромінювання виступає потужність експозиційної дози. На відстані 5 см від поверхні екрану монітору її рівень не повинен перевищувати 100 мкР/год. Максимальний рівень рентгенівського випромінювання на робочому місці програміста зазвичай не перевищує 20 мкР/год.

Таблиця 4.1

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні відеомонітора	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати: для дорослих користувачів	20кВ/м

На відстані 5 – 10 см від екрана і корпусу монітора рівні напруженості можуть досягати 140 В/м по електричній складовій, що значно перевищує допустимі значення.

Електробезпека. Статична електрика. Необхідно враховувати, що будь-який персональний комп’ютер, допоміжне обладнання та периферійні пристрої які експлуатуються разом з ним (принтер, сканер, модем) є електроустановками які живляться напругою до 1000 В. Тому на них і на все, що пов’язано з їх експлуатацією, в повній мірі поширюються вимоги електробезпеки.

З метою забезпечення безпеки, як користувачів, так і обслуговуючого персоналу комп’ютерів, при їх експлуатації в приміщеннях, обладнаних комп’ютерами, повинні бути повністю дотримані вимоги електробезпеки.

Приміщення програмістів за небезпекою ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, без пилу, з нормальною температурою повітря, ізольованими підлогами і малим числом заземлених приладів).

На робочому місці програміста з всього устаткування металевим є лише корпус системного блоку комп'ютера, але тут використовуються системні блоки, що відповідають стандартові фірми IBM, у яких крім робочої ізоляції передбачений елемент для заземлення і провід з жилою, що заземлює, для приєднання до джерела живлення.

Основні причини ураження людини електричним струмом на робочому місці:

– дотик до металевих неструмоведучих частин (корпусу, периферії комп'ютера), що можуть виявитися під напругою в результаті ушкодження ізоляції;

– нерегламентоване використання електричних приладів;

– відсутність інструктажу співробітників з правил електробезпеки.

Під час роботи на корпусі комп'ютера накопичується статична електрика. На відстані 5 – 10 см від екрана напруженість електростатичного поля складає 60–280 кВ/м, тобто в 10 разів перевищує норму 20 кВ/м.

Аналіз техногенних небезпек, вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях. Надзвичайна ситуація – порушення нормальних умов життя і діяльності людей на об'єкті або території, спричинене аварією, катастрофою, стихійним лихом, епідемією, епізоотією, епіфітотією, великою пожежею, застосуванням засобів ураження, що призвели або можуть призвести до людських і матеріальних втрат.

Система забезпечення пожежної безпеки об'єкта захисту включає в себе: систему запобігання пожежі, систему протипожежного захисту, комплекс організаційно-технічних заходів щодо забезпечення пожежної безпеки.

Відповідно до чинного законодавства відповідальність за забезпечення

пожежної безпеки установи несе персонально його керівник.

У рамках даних повноважень керівник закладу зобов'язаний:

– організувати вивчення та забезпечити виконання правил пожежної безпеки усіма працівниками установи;

– встановити на території, у будинках і спорудах установи строгий протипожежний режим. Забезпечити дотримання його всіма керівниками структурних підрозділів, інженерно-технічними працівниками, обслуговуючим персоналом;

– щорічно розробляти конкретні плани практичних заходів щодо підвищення рівня протипожежного захисту установи;

– включати в плани вдосконалення матеріально-технічної бази закладу протипожежні заходи.

Безпосередньо організація роботи з протипожежної безпеки в установі наказом керівника покладається на інженера (старшого інженера) з пожежної безпеки. При відсутності у штаті установи зазначеній посаді обов'язки з пожежної безпеки покладаються на інженера (спеціаліста) з охорони праці з відповідною виплатою компенсації.

Інженер (старший інженер) з пожежної безпеки керує пожежно-профілактичною роботою, контролює дотримання чинних правил і норм з пожежної безпеки, а також встановленого протипожежного режиму в установі. Він підпорядковується безпосередньо керівнику установи та виконує наступні функціональні обов'язки:

– розробляє і веде документацію з пожежної безпеки;

– вносить пропозиції в плани роботи установи щодо забезпечення пожежної безпеки;

– бере участь у розробці інструкцій з пожежної безпеки;

– погоджує інструкції про заходи пожежної безпеки структурних підрозділів установи;

– проводить вступний протипожежний інструктаж з усіма знову прийнятими на постійну і тимчасову роботу;

– контролює проведення протипожежних інструктажів та занять з пожежно-технічного мінімуму.

Крім цього інженер з пожежної безпеки установи бере участь у розгляді проектної документації на будівництво, реконструкцію та капітальний ремонт лабораторних, виробничих, складських та інших приміщень з метою визначення її відповідності вимогам норм і правил пожежної безпеки.

Ступінь вогнестійкості будинків приймається в залежності від їхнього призначення, категорії вибухопожежної і пожежної небезпеки, кількості поверхів, площі поверхів.

По конструктивних характеристиках будинок можна віднести до будинків з несучими і огороджуючими конструкціями із природних або штучних кам'яних матеріалів, бетону або залізобетону, де для перекриттів допускається використання дерев'яних конструкцій, захищених штукатуркою або важкогорючими листовими, а також плитними матеріалами.

Отже, ступінь вогнестійкості будинку можна визначити як третю (III). Приміщення лабораторії по функціональній пожежній небезпеці відноситься до класу Ф 4.2.

Небезпеки пов'язані з порушенням правил пожежної безпеки, хибним визначенням видів та кількості первинних засобів пожежогасіння відносно категорій приміщень с пожежної безпеки.

Також необхідно враховувати, що різні по природі своєї дії небезпечні і шкідливі виробничі фактори можуть проявлятися одночасно. Для профілактики пожежі надзвичайно важлива правильна оцінка пожежонебезпеки будинку, визначення небезпечних факторів і обґрунтування способів і засобів пожежопопередження і захисту.

Одне з умов забезпечення пожежобезпеки – ліквідація можливих джерел запалення. З метою запобігання пожежі пропоную проводити з інженерами-програмістами протипожежний інструктаж, на якому

ознайомити працівників із правилами протипожежної безпеки, а також навчити використанню первинних засобів пожежогасіння.

У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефоні пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації, приведеному на рис. 4.1 і приступити до ліквідації пожежі вогнегасниками. При наявності невеликого вогнища полум'я, можна скористатися підручними засобами з метою припинення доступу повітря до об'єкта загоряння.

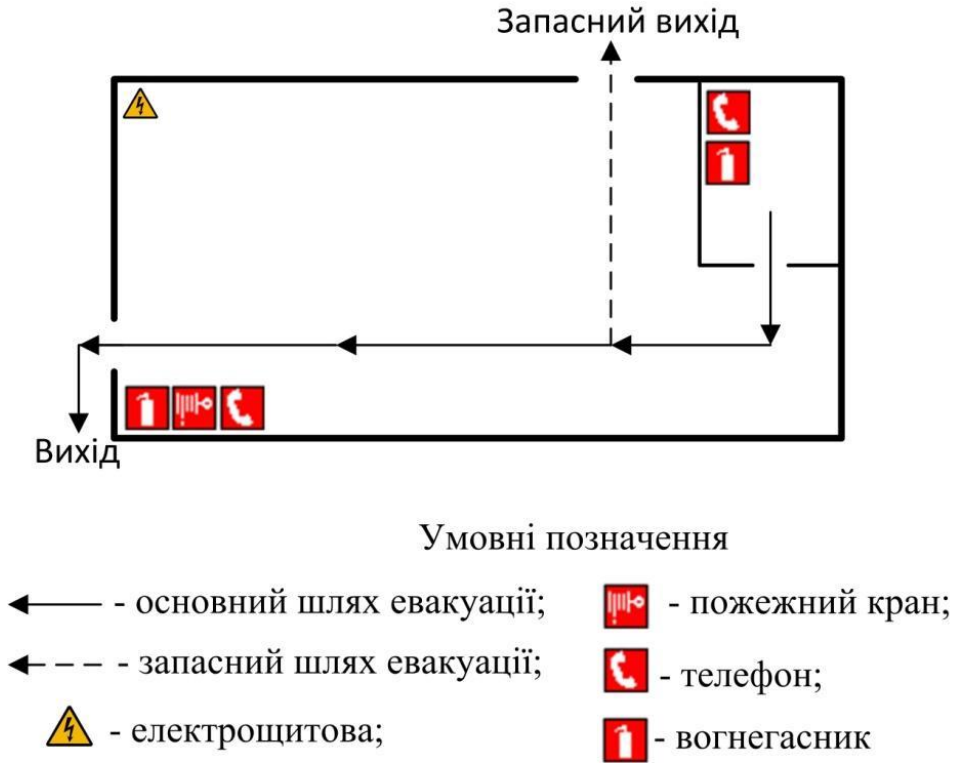


Рисунок 4.1. План евакуації з приміщення лабораторії під час пожежі

Проектування системи штучного освітлення. Трудова діяльність інженера-програміста завжди пов'язана із навантаженням органів зору, оскільки зображення на моніторі складаються з окремих світлових точок різного кольору, яким притаманне також і мерехтіння. При недотриманні вимого охорони праці у працівника неминуче погіршується зір, з'являється головний біль, втома, виникає сльозотеча.

Важливу роль у профілактиці захворювань органів зору відіграє виробниче освітлення на робочому місці. В цілому освітлення – це спрямовування світлової енергії сонця і штучних джерел світла на поверхню предметів для забезпечення зорового сприйняття цих предметів і довкілля. Виробниче освітлення генерує сприятливі психофізіологічні ефекти, позитивно впливаючи на працездатність людини і на створення комфортних і безпечних умов праці. Раціональне освітлення робочих місць є показником високого рівня культури праці. Освітлення для людини є важливим біологічним стимулятором. Його недостатній рівень підвищує втому зорового аналізатора у процесі праці роботи, чим сприяє погіршенню загального стану здоров'я.

Спроектуємо систему штучного освітлення в приміщенні, яке має загальну площу 44 м^2, висоту стелі 3,8 м.

Вихідні дані для проектування системи штучного освітлення:

– фактична виміряна освітленість на поверхні столу: $E_ф$ = 255 лк;

– розміри приміщення: довжина A = 8,8 м; ширина B = 5,0 м;

– розрахункова висота підвісу світильників: H = 3,8 м;

– найменший розмір об'єкта розрізнення для монітора SVGA: 0,26 мм;

– контраст об'єкта розрізнення з фоном – середній

– характеристика фону – світлий;

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

– коефіцієнти відображення: 0,7 – 0,35 – 0,5.

Розряд зорової роботи в даному приміщенні обираємо: II розряд, роботи підвищеної точності [3]. Для II розряду зорової роботи задана норма освітленості на робочому місці: $E_н$ = 500 лк. Робимо висновок, що фактична освітленість на робочих місцях $E_ф$ = 250 лк вдвічи менша за нормативну освітленість. Тому існує необхідність в встановленні більш потужної і ефективної системи освітлення.

Спроектуємо систему загального освітлення, для якої обираємо світильники моделі ЛВП02-4Х80, в яких розміщують чотири

люмінесцентних лампи потужністю 60 Вт. Люмінесцентні лампи застосовують в приміщеннях з підвищеними вимогами до передачі кольору при розміщенні світильників на висоті до 4 м, що відповідає умовам зорової роботи підвищеної точності.

Площа приміщення:

$$S = AB = 8{,}8 \cdot 5{,}0 = 44 \text{ м}^2$$

Індекс приміщення:

$$i = \frac{S}{(A+B) \cdot H} = \frac{44}{(8{,}5+5{,}0) \cdot 3{,}8} = 0{,}86$$

Еквівалентна площа:

$$S_e = \frac{S \cdot K \cdot z}{\eta} = \frac{44 \cdot 1{,}28 \cdot 0{,}5}{0{,}33} = 85{,}3 \text{ м}^2.$$

Попередня розрахункова кількість світильників:

$$N_o = \frac{S_e}{L_o^{\,2}} = \frac{85{,}3}{3{,}5^2} = 6{,}9 \text{ шт.}$$

Приймаємо $N_o = 8$ шт.

Потрібний світовий потік світильника:

$$\Phi_c = \frac{S_e \cdot E_н}{N_o} = \frac{85{,}3 \cdot 500}{8} = 5340 \text{ лм.}$$

Освітленість E_1, яка створюється одним світильником:

$$E_1 = \frac{\Phi}{S_e} = \frac{5340}{85{,}3} = 63 \text{ лк.}$$

Кількість світильників:

$$N_n = \frac{E_н}{E_1} = \frac{500}{63} = 7{,}9 \text{ шт.}$$

Приймаємо остаточну кількість світильників для монтажу $N = 8$ шт. Оскільки попереднє розрахункове значення співпадає із остаточним, розрахунок виконаний вірно.

Таким чином, в приміщенні із робочими місцями інженерів-програмістів необхідно встановити 8 світильників моделі ЛВП02-4Х80,

оснащених чотирма люмінесцентними лампами. Світильники оптимально рівномірно розташувати на стелі в два ряди.

ВИСНОВКИ

Проведено огляд сучасних методів виявлення порушення цілісності цифрового зображення.

Обґрунтовано вибір алгоритмів виявлення порушень цілісності для їх реалізації: алгоритм виявлення клонування, розмиття та масштабування, засновані на аналізі сингулярних чисел блоків матриці цифрового зображення.

Проаналізовано та покращено алгоритм виявлення масштабування цифрового зображення. Введене покращення дозволило скоротити кількість помилок другого роду.

Розроблено програмний продукт, що є інтуїтивно зрозумілий та простий у використанні.

Усі задачі, поставлені в роботі, вирішено. Мету досягнуто.

ПЕРЕЛІК ПОСИЛАНЬ

1. Берія Д.Ю. Зоріло.В.В. Комплексна перевірка електронних файлів підприємства на наявність порушень їх цілісності. *Праці І міжнародної науково-практичної конференції «Підприємство та логістика в умовах сучасних викликі*в». Тернопіль, 2020. – С.67-69.
2. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. К. : ЮНИОР, 2003. 505 с.
3. Нариманова Е.В. Проверка целостности цифрового сигнала. Донецк: Цифровая типография, 2011. 180 с.
4. 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.
5. Грибунин В.Г., Оков И.Н. , Туринцев И.В. Цифровая стеганография . М. : СОЛОН-Пресс, 2002. 272 с.
6. Fridrich J. Methods for Tamper Detection in Digital Images. *ACM MM&SEC 1999: Proceedings of the Multimedia and Security Workshop 1999*,. — Orlando, Florida, USA, 1999. P..19—23.

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

8. Fridrich J,. Goljan M. Images with self-correcting capabilities. ICIP *1999: Proceedings of IEEE International Conference on Image Processing,* Kobe, Japan, 1999. . Vol.3. P. 792—796.

9. Yeung M.M. Mintzer F. An Invisible Watermarking Technique for Image Verification . ICIP 1997: Proceedings of IEEE International Conference on Image Processing,. Santa Barbara, California, USA, 1997. Vol.2. P. 680—683.

10. Wolfgang R. B. Delp E. J. A Watermark for Digital Images. *ICIP 1996: Proceedings of IEEE International Conference on Image Processing*, Lausanne, Switzerland, 1996. Vol.3. P. 219—222.

11. Dybala B Jennings B., Letscher D. Detecting filtered cloning in digital images. *ACM Multimedia and Security Workshop*. 2007. P. 43–50.

12. Langille A. Gong M. An efficient match-based duplication detection algorithm. *Canadian Conference on Computer and Robot Visi*on. 2006 P.64.

13. Luo W.. Huang J.,. Qiu G. Robust detection of region duplication forgery in digital images. *International Conference on Pattern Recognition*. 2006. P.746–749.

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

15. Wang J., Liu G., Li H., Dai Y., Wang Z. Detection of image region duplication forgery using model with circle block. *International Conference on Multimedia Information Networking and Securit*y. 2009. 25–29.

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

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

18. Трифонова Е. А., Килин А. Е. Метод локализации и идентификации

контекстно-зависимого масштабирования в цифровом изображении. *МНПК «Современные информационные и электронные технологии»*. Одесса, 26–30 мая 2014 г. С. 117–118.

19. Трифонова К. О. Метод локализации и идентификации масштабирования в цифровом изображении. *Інформатика та математичні методи в моделюванні*, 2013. Т. 3, №1, с. 22–34.

20. Amerini I, Ballan L., Caldelli R., Del Bimbo A., Serra G A sift-based forensic method for copymove attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security*.2011. 6(3):1099–1110.

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

22. Popescu A.C. Farid H. Statistical tools for digital forensics. *The 6th International Workshop on Information Hiding*, Toronto, Canada, 2004. P. 128—147.

23. Johnson M.K., Farid H.. Exposing digital forgeries by detecting inconsistencies in lighting. *ACM Multimedia and Security Workshop*, New York, NY, 2005.

24. Нариманова Е.В. Достаточные условия проявления эффекта двойного квантования. *Тр. Одес. политехн.ун-та*. 2008. №2(30). С. 166—169.

25. Fan J. Kot A.C., Cao H., Sattar F. Modeling the exif-image correlation for image manipulation detection. *International Conference on Image Processing*. 2011. P.1945-1948.

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

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

28. 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.

29. 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.

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

31. 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. С.69.

32. Кобозева А.А. Использование особенностей возмущения сингулярних чисел матрицы цифрового изображения для обнаружения его фальсификации *Искусственный интеллект*. 2008. №1. С.145—153.

33. Кобозева А.А.,Трифоноват Е.А. Повышение эффективности метода обнаружения фальсификации цифрового изображения, основанного на анализе сингулярных чисел матрицы. *Тр. Одес. политехн.ун-та*. 2008. №1(29). С. 183–190.

34. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах. *Вісник Східноукраїнського національного університету ім. Володимира Даля* . 2006. №9(103), ч.1. .С.74.

35. Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации . *Искусственный интеллект*. 2007. №4. С.531-538.

36. Зорило В.В. Выявление клонирования как фальсификации цифрового изображения. *Вісник Національного технічного університету «ХПІ». Збірник*

наукових праць. Тематичний випуск «Системний аналіз, управління та інформаційні технології». Х.: НТУ «ХПІ», 2011. № 35 С.. 31-38.

37. Зоріло В.В. Метод підвищення ефективності виявлення порушення цілісності цифрового зображення: Дисертаційна робота кандидата технічних наук: 05.13.21. К., 2013. 127с.

Хореев, П.Б. Способы и средства защиты информации. М.: МО РФ, 2000. 316 с.

1. Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроям [Електронний ресурс] : НПАОП 0.00-7.15-18. – На заміну НПАОП 0.00-1.28-10 ; чинний від 2018-05-18. – К. : Мінсоцполітики України, 2018. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0508-18. – (Нормативно-правовий акт охорони праці)

2. Санітарні норми мікроклімату виробничих приміщень [Електронний ресурс] : ДСН 3.3.6.042-99. – Чинний від 1999-12-01. – К. : МОЗ України, 1999. – URL: http://zakon2.rada.gov.ua/rada/show/va042282-99. – (Державні санітарні норми)

3. Природне і штучне освітлення. [Текст] : ДБН В.2.5-28-2018. – На заміну ДБН В.2.5-28-2006 ; чинний з 2019-03-01. – К. : Мінрегіон України, 2018. – 133 с. – (Державні будівельні норми України)

4. Правила пожежної безпеки в Україні [Текст] : НАПБ А.01.001-14. – На заміну НАПБ А.01.001-04 ; чинний від 2014-12-30. – К. : МВС України, 2014. – 47 с. – (Нормативний акт пожежної безпеки)