Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму

Виконав: ст. 2-го курсу, групи УБ-21мз
спеціальності 125– Кібербезпека
Освітня програма – Управління
інформаційною безпекою
Іщенко Юрій Петрович
Керівник: к.т.н., доц., доцент каф. МБІС
Карпінець В.В.
«14» червня 2023 р.
Опонент: к.т.н., доц., доцент каф. ОТ
Савицька Л.А.
«14» червня 2023 р.

Допущено до захисту
Голова секції УБ кафедри МБІС

Юрій ЯРЕМЧУК
“14” червня 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітньо-професійна програма – Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС

Юрій ЯРЕМЧУК

«22» березня 2023 р.

З А В Д А Н Н Я

на магістерську кваліфікаційну роботу студенту

Іщенку Юрію Петровичу

1. Тема роботи «Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму». Керівник роботи к.т.н., доц., доцент каф. МБІС Карпінець В.В. затверджені наказом вищого навчального закладу від «20» березня 2023 року № 68

2. Строк подання студентом роботи за тиждень до захисту.

3. Вихідні дані до роботи: нормативно-правова база, монографії та сучасні наукові статті по темі, Інтернет-ресурси, стандарти, існуюче ПЗ.

4. Зміст текстової частини: в першому розділі проаналізувати методи захисту електронних документів від несанкціонованої модифікації; в другому розділі здійснити вдосконалення методу, провести проектування розробки, розробити алгоритми програмної частини; в третьому розділі здійснити програмну реалізацію розробки та аналіз результатів; в четвертому розділі проаналізувати економічну ефективність розробленого програмного забезпечення.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов`язкових креслень): у першому розділі наведено 4 рис., 1 табл.; у другому розділі наведено 9 рис., 1 табл.; у третьому розділі наведено 27 рис., 3 табл.; четвертому розділі наведено 7 рис., 1 табл.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	к.т.н., доц. каф. МБІС Карпінець В.В.		
Економічна частина	к.т.н., доц. каф. ЕПВМ , Ратушняк О.Г.		

7. Дата видачі завдання 22 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку МКР, формулювання теми	22.03.2023	27.03.2023	
2.	Аналіз предметної області обраної теми	28.03.2023	04.04.2023	
3.	Розробка алгоритму роботи	05.04.2023	19.04.2023	
4.	Написання МКР на основі розробленої теми	20.04.2023	15.05.2023	
5.	Розробка економічної частини	16.05.2023	31.05.2023	
6.	Попередній захист МКР	01.06.2023	09.06.2023	
7.	Виправлення, уточнення, коригування роботи	10.06.2023	19.06.2023	
8.	Захист МКР	20.06.2023	21.06.2023	

Студент Іщенко Ю.П.

Керівник роботи Карпінець В.В.

АНОТАЦІЯ

УДК: 004.056

Іщенко Ю.П. Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму. Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Управління інформаційною безпекою». Вінниця: ВНТУ, 2023. 115 с.

На укр. мові. Бібліогр.: 50 назв; рис.: 41; табл. 12.

У магістерській кваліфікаційній роботі представлено підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму.

В першому розділі роботи проведено аналіз застосування ЦВЗ з метою захисту електронних документів від несанкціонованої модифікації, досліджено особливості стеганографічних систем.

У другому розділі роботи описано вдосконалення методу за рахунок застосування дискретного вейвлет-перетворення із використанням модифікованих коефіцієнтів середньочастотної та високочастотної областей, а також додаткового закриття зображення адаптивним шумом.

У третьому розділі роботи здійснено практичну реалізацію програмного додатку на основі вдосконаленого алгоритму. Результати тестування свідчать, про успішність вдосконаленого методу та доцільність його застосування на практиці. Стійкість алгоритму до впливів на стегоконтейнер підвищена орієнтовно на 7%.

У четвертому розділі роботи здійснено аналіз економічної доцільності розробки, який свідчить про її високий комерційний потенціал та доцільність подальшого впровадження.

Ключові слова: цифровий водяний знак, електронні документи, метод RDH, дискретне вейвлет-перевторення, JPEG, PDF.

ABSTRACT

Yuriy Ishchenko. Increasing the stability of the method of protecting electronic documents from unauthorized modification based on an improved RDH (reversible data hiding) algorithm using adaptive noise. Master's qualification work in specialty 125 – «Cyber Security», Education Program «Information Security Management». Vinnytsa: VNTU, 2023. 115 p.

In Ukrainian. Bibliography: 50 titles; Figures: 41; Table 12.

The master's qualification work presents an increase in the stability of the method of protecting electronic documents from unauthorized modification based on an improved RDH algorithm using adaptive noise.

The first section of the paper analyzes the use of RDH to protect electronic documents from unauthorized modification, and investigates the features of steganographic systems.

The second section of the paper describes the improvement of the method by applying the discrete wavelet transform method using modified coefficients of the mid- and high-frequency regions, as well as additional closure of the image with additive noise.

In the third section of the paper, the practical implementation of a software application based on the improved algorithm is carried out. The test results indicate the success of the improved method and the feasibility of its application in practice. The algorithm's robustness to impacts on the stego container has been increased by about 7%.

The fourth section of the paper analyzes the economic feasibility of the development, which indicates its high commercial potential and the feasibility of further implementation.

Keywords: digital watermark, electronic documents, RDH method, discrete wavelet transform, JPEG, PDF.

ЗМІСТ

ВСТУП

Актуальність. З виникненням обчислювальної техніки питання захисту інформації стає дедалі актуальнішим. Одним із її аспектів є захист авторських прав на електронні документи та ресурси. Використовуючи обчислювальні засоби, зловмисники можуть використати та поширювати електронну інформацію. Таким чином, правовласнику завдається і матеріальна, і моральна шкода.

Найефективнішими засобами захисту авторства електронних документів на сьогодні є використання цифрової стеганографії, зокрема, цифрових водяних знаків [1 – 2]. Цифровий водяний знак (ЦВЗ) являє собою дані, що впроваджуються в інформаційний об'єкт з метою контролю його використання. Технологія ЦВЗ заснована на застосуванні стеганографічних прийомів, у рамках яких приховується факт наявності ЦВЗ в інформаційному об'єкті (контейнері).

В даній роботі досліджено метод оборотного приховування даних гістограмного типу. Для розподілу вбудовуваних даних запропоновано застосовувати метод дискретного вейвлет-перетворення із використанням модифікованих коефіцієнтів середньочастотної та високочастотної областей. Щоб ускладнити візуальне сприйняття змін файлу-контейнера під час вбудовування ЦВЗ здійснюється додаткове закриття зображення адаптивним шумом.

Отримані результати тестування програмного додатку свідчать про успішність вдосконаленого методу та доцільність його застосування на практиці. Вдосконалений метод на основі гістограмного типу має вищі якісні та кількісні показники порівняно з початковим методом, а стійкість алгоритму до впливів на стегоконтейнер підвищена орієнтовно на 7%.

Мета і задачі дослідження. Метою роботи є підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму.

Задачами дослідження є:

– аналіз актуальності обраної предметної області;

– аналіз особливостей стеганографічної системи, а також цифрового водяного знаку як засобу захисту даних;

– аналіз існуючих методів вбудовування ЦВЗ та поширених атак на стеганографічні системи;

– здійснення вдосконалення обраного методу захисту електронних документів від несанкціонованої модифікації;

– розробка алгоритму роботи програмного засобу на основі вдосконаленого методу;

– проектування та розробка інтерфейсу користувача та реалізація програмного засобу;

– тестування розробки та аналіз отриманих результатів;

– економічне обґрунтування доцільності впровадження здійсненої розробки на основі вдосконаленого методу вбудовування ЦВЗ.

Об’єкт дослідження – цифровий водяний знак для захисту електронних документів від несанкціонованої модифікації.

Предмет дослідження – процес підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі цифрового водяного знаку.

Наукова новизна: вдосконалення алгоритму RDH з використанням адаптивного шуму з метою підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації.

Практична цінність: розроблено програмний продукт, який реалізує вдосконалений метод вбудовування цифрового водяного знаку у електронні документи з метою їх захисту від несанкціонованої модифікації.

1 ЗАГАЛЬНИЙ АНАЛІЗ ГАЛУЗІ ЗАСТОСУВАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

В даному розділі проведено аналіз обраної предметної галузі, а саме застосування стеганографічних методів захисту інформації. З метою підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації. На етапі аналізу теоретичного матеріалу було досліджено актуальність вивчення обраної галузі, проведено аналіз цифрового водяного знаку як стеганографічного методу захисту інформації, а саме застосування ЦВЗ для захисту електронних документів, проведено аналіз сучасних атак та існуючих методів захисту на основі ЦВЗ із забезпеченням його стійкості до активних та пасивних дій порушника.

1.1 Актуальність дослідження обраної галузі

Останніми роками, як у державних, так і комерційних організаціях дедалі ширше використовується електронний документообіг, у зв'язку з чим проблема захисту електронних документів є досить актуальною (рис. 1.1). Очевидно, що залежно від свого змісту електронні документи мають різний ступінь конфіденційності.

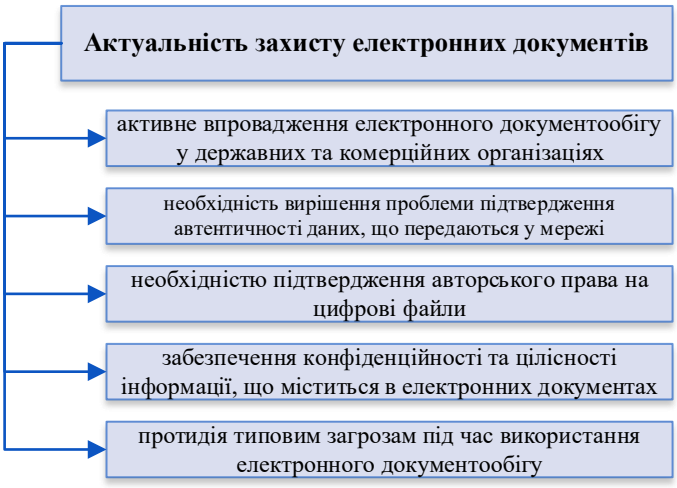


Рисунок 1.1 – Причини актуальності дослідження галузі захисту електронних документів [3 – 4]

Існує також проблема автентичності документів, що передаються в мережі, наприклад, документ, отриманий електронною поштою, не можна засвідчити печаткою або підписати звичайним способом. Тому електронний документообіг необхідно супроводжувати різноманітними організаційними та технічними заходами і засобами для захисту електронних документів від несанкціонованого доступу або модифікації [5].

Загрози для електронних документів є типовими для інформації в електронному вигляді – це загрози цілісності, конфіденційності та доступності. Для протидії типовим загрозам під час використання електронного документообігу має також забезпечуватися збереження документів від втрати та псування і бути можливість їх швидкого відновлення [6 – 7]. Наприклад, системи електронного документообігу, які в основі своїй використовують бази даних Microsoft SQL Server або Oracle, використовують засоби резервного копіювання, вбудовані в ці бази даних.

Забезпечення безпечного доступу до даних всередині системи електронного документообігу здійснюється з використанням аутентифікації та розмежуванням прав користувача.

Найпоширенішими є два методи автентифікації – парольний і майновий. На парольний метод сильно впливає людський фактор – пароль часто виявляється відомим порушнику [8].

Майновий метод надає більший ступінь захисту, для аутентифікації необхідні різні USB-ключі, смарт-картки тощо [9]. Цей метод теж не захищений від людського фактора, однак, крім пароля необхідно мати і пристрій для доступу. У будь-якій системі обов'язково має бути передбачено розмежування прав користувача, і чим гнучкіше і детальніше, тим краще.

Конфіденційність найчастіше забезпечується криптографічними методами. За допомогою них конфіденційність зберігається навіть у разі потрапляння документа до рук зловмисників [10]. Із криптографічними засобами слід звертати увагу і на організаційну складову захисту інформації. Незалежно від криптографічних методів, порушник може отримати доступ до документа за

допомогою комп'ютера з відкритим на ньому документом. Розшифровка інформації також не становить труднощів, якщо не здійснюється контроль ключів у користувачів [11].

Електронно-цифровий підпис (ЕЦП) є основним засобом для забезпечення автентичності документа, отриманого в електронному вигляді. ЕЦП слугує для захисту документа від спотворення, підміни авторства, відмови від авторства. Електронно-цифровий підпис, по суті, є цифровою печаткою, тому що, на відміну від фізичного підпису, він є спільним для підприємства, відділу або комп'ютера [12]. Виходить, що будь-яка людина, яка має доступ до ресурсів, що відповідають за створення та інші дії з ЕЦП, може вчинити такі протиправні дії:

– змінити вихідний документ, після чого згенерувати новий ЕЦП;

– змінити авторство документа, у підсумку привласнивши собі чужий документ, або надіслати свій документ під чужим ім'ям;

– знищити вихідний документ, надіслати інший документ замість вихідного.

Таким чином, через таких порушників під загрозою опиняється не тільки цілісність документа, але також і авторство.

Для захисту документа від подібного роду впливів рекомендується використовувати, крім ЕЦП, й інші засоби, фактично об'єднуючи криптографічні та стеганографічні методи захисту.

Одним із таких засобів може слугувати цифровий водяний знак (ЦВЗ) – спеціальна мітка, що вбудовується в контейнер з метою захисту авторських прав і підтвердження цілісності контенту [13].

ЦВЗ застосовуються для захисту від несанкціонованого використання та копіювання документів, за допомогою ЦВЗ можливо відстежити порушника, який створює неправомірні копії. Система вбудовування ЦВЗ повинна запобігати спробам зловмисників змінювати цифровий водяний знак і вихідні дані в контейнері.

1.2 Аналіз застосування цифрової стеганографії

Цифрова стеганографія – це розділ стеганографії, що вивчає надійне приховування певних бітових послідовностей в стеганоконтейнерах (фото, документи, аудіо-файли). В такій системі непомітність передбачає включення людини в стегосистему, а надійність – це стійкість до спотворень різних видів. В такій системі людина розглядається як додатковий приймач інформації, що може пропонувати до стегосистеми важко формалізовані вимоги. Разом з тим, напрямок стеганографії як засб захисту інформації має широке застосування у багатьох галузях (табл. 1.1.).

Таблиця 1.1 – Галузі застосування стеганографії

Мета захисту	Галузь застосування
Захист від копіювання [14]	Електронна комерція, контроль за копіюванням DVD, розповсюдження мультимедійної інформації
Прихована анотація документів [15]	Медичні знімки, картографія, мультимедійні база даних
Аутентифікація [16]	Системи відеоспостереження, електронні комерції, голосова пошта, електронне конфіденційне діловодство
Прихований зв'язок [17]	Воєнні та розвідувальні додатки, а також застосування у випадках, коли неможливе застосування криптографічних методів

За останні декілька років стеганографія набуває все більшого поширення у різних сферах життя людини, у зв’язку з цим сформовано такі її напрями [18]:

– вбудовування інформації з метою її передачі;

– вбудовування цифрових водяних знаків;

– вбудовування ідентифікаційних номерів;

– вбудовування заголовків.

Основні переваги цифрової стеганографії полягають у тому, що вона забезпечує конфіденційність, оскільки вбудована інформація може бути захована в незначних змінах, які важко помітити без спеціального аналізу, а також відсутність видимого зміни в оригінальному файлі забезпечує

незалежність від детекторів інших методів аналізу, таких як антивірусні програми [19].

Однак важливо враховувати, що стеганографія не забезпечує шифрування даних. Вона лише приховує наявність додаткової інформації, але не захищає її від розшифрування або злому. Крім того, деякі методи стеганографії можуть впливати на якість файлу, особливо при вбудовуванні великих обсягів даних.

Загальну структуру стеганографічної системи для вбудовування цифрового водяного знаку у електронні документи можна представити у вигляді схеми (рис. 1.2).

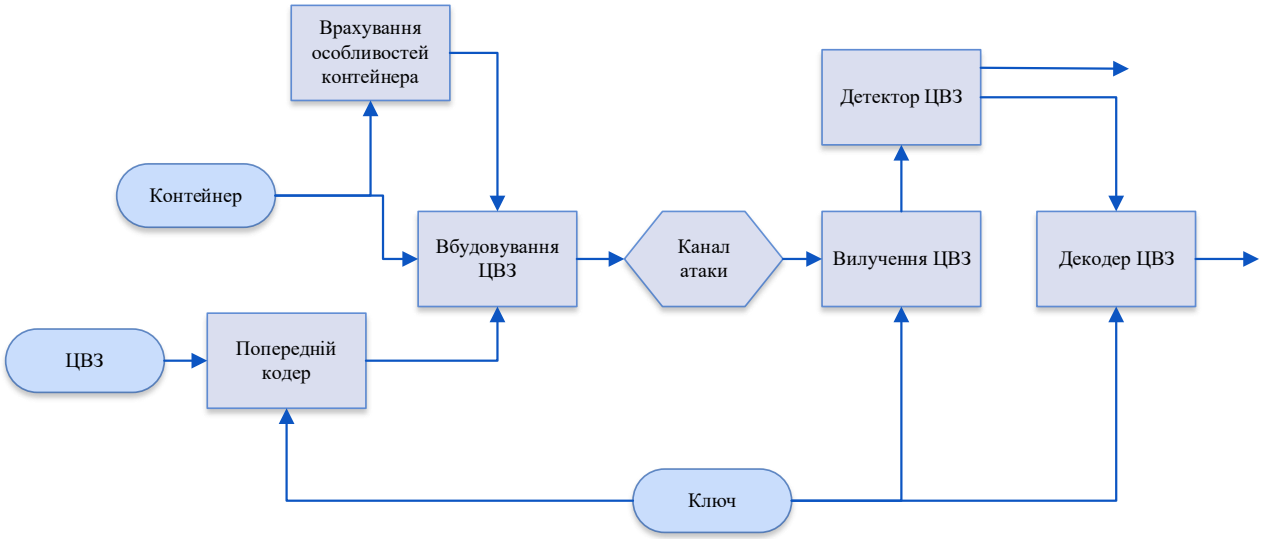


Рисунок 1.2 – Структурна схема цифрової стеганографічної системи [20]

Представлена на рис. 1.2 схема демонструє стеганографічну систему, що-має на мені виконання функції вбудовування та зчитування прихованого цифрового водяного знаку із стегоконтейнера. В такій стеганографічній системі здійснюється злиття двох типів даних з метою неможливості виявлення різними детекторами (наприклад, зорова система людини та система виявлення ЦВЗ). Для збільшення надійності приховування інформації застосовується ключ, після формування якого відбувається вбудовування ЦВЗ. Виявлення ЦВЗ у захищеному контейнері реалізується за допомогою декодера.

Цифровий водяний знак (ЦВЗ) являє собою дані, що впроваджуються в інформаційний об'єкт з метою контролю його використання [21]. Технологія

ЦВЗ заснована на застосуванні стеганографічних прийомів, у рамках яких приховується факт наявності ЦВЗ в інформаційному об'єкті (контейнері). Проте, в ньому зберігатиметься інформація, що може бути зчитана з даного контейнера при наявності відповідного стеганографічного ключа, що визначатиме права доступу до елементів цифрового водяного знаку.

Сьогодні, цифрові водяні знаки активно застосовуються для здійснення контролю за використанням мультимедійного контенту, електронних документів.

Суттєва особливість файлів-контейнерів мультимедійного контенту полягає в тому, що всі вони є пасивними інформаційними об'єктами, що виконують тільки функцію зберігання даних. Очевидно, що необхідність у контролі використання інформаційних об'єктів не обмежується тільки контейнерами цього виду.

Така необхідність має місце і для активних інформаційних об'єктів які виконують деяку обчислювальну або керівну функцію.

1.3 Аналіз застосування ЦВЗ для захисту електронних документів

Для захисту паперових або електронних документів нині використовують різні методи і технології, включно з методами криптографічного захисту та електронного цифрового підпису.

Одним із перспективних методів захисту, що відповідає вимогам конфіденційності та, водночас, мінімальних часових і вартісних витрат, є метод стеганографічного приховування інформації (СЗІ) [22], який у застосуванні до завдань захисту документів реалізує застосування технологій цифрових водяних знаків (ЦВЗ), що отримали свою назву за аналогією з паперовими водяними знаками. В основі цих технологій лежить впровадження в об'єкт цифрового контенту стеганографічно-прихованих і захищених від модифікації даних, які тим чи іншим чином маркують цей об'єкт.

У разі несанкціонованого використання, поширення об'єкта або його підміни, а також фальсифікації будь-якої його частини наявність або відсутність

ЦВЗ дає змогу ідентифікувати ситуацію, що виникає.

Нині технології ЦВЗ розвивають для захисту авторських прав на дані та документи, представлені в електронному вигляді. ЦВЗ бувають різних типів. Перш за все, розрізняють невидимі та видимі ЦВЗ.

Невидимі ЦВЗ вбудовуються таким чином, щоб користувач не здогадувався про наявність даних, що підтверджують авторство або справжність електронного об'єкта захисту [23]. Файли, що захищаються, у цьому разі виступають у ролі контейнера, що зберігає ЦВЗ у прихованій формі, недоступній для стороннього спостерігача.

Як вбудовані дані зазвичай виступає послідовність даних, що містять кодовану інформацію ЦВЗ.

Як видимі ЦВЗ виступають логотипи і всілякі маркування, а також інша інформація, що ідентифікує автора документа або справжність. Такі ЦВЗ мають головний недолік, який полягає в тому, що їх можна підробити або зовсім видалити [24].

Враховуючи особливості систем вбудовування цифрового водяного знаку, проаналізуємо типи атак, що можуть на них здійснюватись.

Оскільки вивчення особливостей таких атак надасть можливість якісніше сформувати алгоритм вбудовування ЦВЗ та зробити його реалізацію більш практичною. Виходячи із проаналізованого матеріалу, можна виокремити такі групи атак на ЦВЗ (рис. 1.3).

Варто зауважити, що дану класифікацію атак не слід вважати повною, оскільки можливі різні види комбінації загроз, а певні типи атак (наприклад, такі як видалення шуму) можуть бути віднесені до різних категорій.

Розглянемо ситуацію, коли захист цифрової фотографії здійснюють з метою доведення її незаконного використання або можливої фальсифікації. У цьому випадку вихідне зображення може бути піддано низці зовнішніх впливів (атак), до яких відносяться зашумлення, обрізка країв зображення, кадрування, фільтрація, повороти, зміна цифрового формату, стиснення з втратами і масштабування.

Рисунок 1.3 – Типи атак на стеганографічні системи ЦВЗ [25 – 26]

Також будь-які фрагменти захищеної фотографії можуть бути додані або, навпаки, видалені. Частина цих впливів, таких, як зашумлення або фільтрація, спрямована безпосередньо на вилучення або пошкодження можливих вбудованих міток; інші, наприклад, кадрування, масштабування, спрямовані на підготовку зображення до його комерційного використання.

Проте, на сьогодні існують різні методи захисту від вищенаведених атак, а з урахуванням мети застосування ЦВЗ обирають найбільш доречний для роботи метод.

Аналіз існуючих методів захисту електронних документів на основі цифрових водяних знаків здійснимо в наступному підрозділі.

1.4 Аналіз існуючих методів захисту електронних документів

Застосування технологій ЦВЗ для захисту електронних і паперових документів має свою специфіку, пов'язану з формою подання текстових даних. Основними вимогами, що висуваються до ЦВЗ, у цьому плані є можливість реалізації технологій вбудовування і вилучення ЦВЗ без використання спеціального обладнання (мінімальні фінансові витрати), забезпечення необхідної місткості (пропускної спроможності) контейнера ЦВЗ, захищеність від підробки і знищення ЦВЗ, стійкість до цифро-аналогових і аналого-цифрових перетворень (для паперових документів).

Узагальнений алгоритм вбудовування цифрових водяних знаків може бути представлений у вигляді математичної моделі побудови алгоритмів, стійких до цифро-аналогових перетворень завдяки врахуванню параметрів друкарського і скануючого пристрою (роздільна здатність). Модель дає змогу визначити такі основні параметри конкретної стегосистеми, як тип декодера, тип ключа, вимоги до ЦВЗ, вимоги до зображення-контейнера [27].

Розглянемо з погляду висунутих вимог відомі результати в галузі створення невидимих і видимих ЦВЗ в інтересах захисту електронних і паперових документів.

Стандартними і досить тривіальними методами створення невидимих ЦВЗ в електронних текстових документах є методи, що ґрунтуються на маніпуляції під час розставлення переносів, табуляцій або пропусків у тексті, а також вбудовування ЦВЗ у порожнечі й керувальні елементи файлів, дисків і мережевих пакетів (нижчий рівень архітектури). Незважаючи на очевидну простоту і дешевизну таких алгоритмів, у них є один великий недолік: за будь-якого переформатування тексту відбувається втрата даних ЦВЗ.

Широке застосування з метою посвідчення особи й аутентифікації та під час прихованого передавання інформації в паперових документах дістала стегосистема «Invisible Personal Information» [28]. Вбудовування ЦВЗ у цій системі здійснюється шляхом малого зсуву всіх обраних точок контейнера на

однакову величину в одному напрямку. Принцип вилучення ЦВЗ полягає в накладенні на зображення-контейнер лінзового растра, сітка якого збігається з вихідним зображенням, тоді в місцях зсуву відбудеться зміна середньої яскравості. середньої яскравості і ЦВЗ буде видно.

Ще один універсальний спосіб формування невидимих ЦВЗ полягає в зсуві деяких обраних пікселів щодо центру зображення. Документ розбивається на рядки, у кожному з яких може бути обраний тільки один піксель. Для вбудовування «0» обирають піксель із координатами лівіше від центру, а для вбудовування «1» - правіше.

Наступний метод приховування інформації заснований на властивості гліфів різних кодувань. Інформацію вносять заміною окремих символів тексту символами того самого кодування, але іншого алфавіту, що відповідають за зовнішнім відображенням, унаслідок чого текст матиме різне двійкове представлення без видимих візуальних ознак.

До видимих методів належать різні види поліграфічного захисту: дизайн, друк, використання спеціального паперу, фарб та оздоблення, а також вбудовування штрихових кодів.

Ще один метод вбудовування ЦВЗ являє собою технологію маркерів автентичності. Технологія дає можливість створювати ЦВЗ, що забезпечує перевірку авторства і змісту документа. Цей ЦВЗ має вигляд структурованої матриці-зображення з квазіперіодичною структурою, що складається з із чорних і білих елементів (ЦВЗ формується з використанням методу двовимірного матричного кодування, що має високу пропускну здатність). Зміст документа архівують, доповнюють ЕЦП і сертифікатом відкритого ключа (для перевірки справжності підпису) і вбудовують у маркер. У разі розбіжності змісту маркера і документа, документ вважається підробкою [29].

Окрім того, на сьогодні запропоновано безліч методів вбудовування інформації в зображення. Наприклад, розроблено такі просторові методи, як: метод LSB (Last Significant Bit); метод випадкового інтервалу; метод псевдовипадкової перестановки (вибору); метод блочного приховування [30].

Метод заміни найменш значущого біта (Least Significant Bit, LSB) є одним з найпоширеніших методів цифрової стеганографії. Він базується на теорії, що найменш значущі біти в цифрових даних (наприклад, пікселях зображення або відтінках звукового сигналу) мають менший вплив на сприйняття змісту медіа-файлу людиною.

Процес вбудовування інформації за допомогою методу LSB включає наступні кроки:

– вибір медіа-файлу: Обирається цифровий медіа-файл, який буде використовуватися для приховування інформації (наприклад, зображення у форматі BMP або звуковий файл у форматі WAV).

– конвертація інформації: якщо необхідна, інформація, яку потрібно приховати, перетворюється у відповідний формат (наприклад, текстовий рядок перетворюється на бітову послідовність).

– вбудовування інформації: Для кожного байта (або кожного пікселя) медіа-файлу виконується заміна його найменш значущого біта на біт інформації, яку необхідно приховати. Цей процес повторюється для кожного байта (пікселя) медіа-файлу, доки вся інформація не буде вбудована.

– збереження зміненого медіа-файлу: Оновлений медіа-файл, який містить вбудовану інформацію, зберігається.

При розшифруванні або вилученні прихованої інформації процес виконується в зворотному напрямку: найменш значущі біти кожного байта (пікселя) зміненого медіа-файлу зчитуються і складаються разом.

Основними перевагами цього методу є [30]:

– непомітність для людської зорової системи змін в молодших бітах;

– простота реалізації ідеї самого методу;

– можливість приховувати у відносно невеликих зображеннях досить великі обсяги інформації.

Основний недолік методу LSB полягає у його високій чутливості до спотворень контейнера. Для усунення даного недоліку здебільшого використовують завадостійке кодування. Проте, окрім цього, описаний метод

має низьку стеганографічну стійкість до атак пасивних та активних дій порушника.

Наступний метод випадкового інтервалу на відміну попередньо розглянутого методу LSB надає можливість здійснювати випадковий розподіл бітів вбудовуваного повідомлення за контейнером, у результаті чого відстань між двома вбудованими бітами приховуваного повідомлення буде визначена випадковим чином [30]. Недолік даного методу полягає у тому, що біти прихованого повідомлення в контейнері розміщуються в тій самій послідовності, що і в самому прихованому повідомленні. Для усунення даного недоліку застосовують метод псевдовипадкової перестановки, що полягає у використані генератора псевдовипадкових чисел на основі якого генерується послідовність індексів $j_1, j_2, \dots j_k$, та виконується збереження $k-$ го біта повідомлення в пікселі з індексом j_k.

Наступний метод блокового приховування [30] працює наступним чином: зображення-оригінал розбивається на l_m блоків, що не перетинаються, $\Delta i (1 \leq i \leq l_m)$ довільної конфігурації, для кожного з них обчислюється біт парності $b(\Delta i) = \sum_{j \in \Delta_i}^{mod\ 2} LSB(C_j)$. У кожному блоці здійснюється приховування одного секретного біта M_i. Якщо біт парності $b(\Delta i) \neq M_i$, то реалізується інвертування одного з найменших значущих бітів блоку Δi, в результаті чого $b(\Delta i) = M_i$. Вибір блоку може здійснюватись псевдовипадковим чином з використанням стеганографічного ключа. Власне, описаний метод характеризується аналогічною стійкість до спотворень, що й методи, описані вище, проте порівняно з ними, він має певні переваги, зокрема, це можливість модифікації значення такого пікселя в блоці, зміна якого призведе до мінімальної зміни статистики контейнера, а також вплив наслідків вбудовування секретних даних у контейнер можна зменшити завдяки збільшенню розміру блоку.

Наступним методом, що варто розглянути в даній роботі – це Patch-Work [30], за алгоритмом якого спочатку псевдовипадковим чином відповідно до ключа обирається два пікселі зображення. Потім значення яскравості одного з них збільшують на певну величину (від 1 до 5), іншого – зменшують на ту саму

величину. Дана операція повторюється багаторазово (близько 10 тисяч разів), далі потрібно знайти суму значень усіх різниць:

$$S_n = \sum_{i=1}^{n}\big((a_i + c) - (b_i - c)\big) = 2cn + \sum_{i=1}^{n}(a_i - b_i),$$

де a_i і b_i – значення яскравості двох обраних пікселів на кроці i, c – величина приросту, на яку зміняться яскравість на кожному кроці алгоритму.

Математичне очікування суми різниць значень яскравості пікселів у незаповненому контейнері $\sum_{i=1}^{n}(a_i - b_i)$ близька до нуля при досить великому значенні n. Таким чином, за наявності ЦВЗ величина S_n значно більша за нуль.

Основна перевага даного методу – це достатня стійкість до операцій стиснення, усічення і зміни контрастності зображення. До недоліків методу належить його нестійкість до афінних перетворень (повороту, зсуву, масштабування), а також його мала пропускна спроможність (для передавання 1 біта прихованого повідомлення потрібно 20 тисяч пікселів).

Найбільш поширені на сьогодні методи вбудовування ЦВЗ наведені на рис. 1.4.

Рисунок 1.4 – Поширені методи вбудовування ЦВЗ у електронні файли [30]

Загалом можна зробити висновок, що наявні на даний момент методи й алгоритми, здебільшого, не можна застосовувати як засоби універсального захисту різних типів документів, оскільки вони ґрунтуються на індивідуальних особливостях кожного типу контенейра (наприклад, особливостях двійкового представлення даних або спеціальних фарб, паперу та ін.).

Вирішення проблеми створення універсального методу внесення ЦВЗ для захисту електронних документів потребує подальшого розвитку та буде досліджено у даній роботі.

1.5 Висновки та постановка задач

Отже, в даному розділі було здійснено аналіз стеганографічної галузі та її методів з метою захисту даних, що містяться в електронному документообороті.

Актуальність дослідження даної галузі зумовлена необхідністю вирішення проблеми підтвердження автентичності даних, що передаються у мережі, необхідністю підтвердження авторського права на цифрові файли, метою забезпечення конфіденційності та цілісності інформації, що міститься в електронних документах, а також з метою протидії типовим загрозам під час використання електронного документообігу.

В ході написання даного розділу було здійснено аналіз застосування цифрового водяного знаку з метою захисту електронних документів від несанкціонованої модифікації, досліджено особливості стеганографічних систем, здійснено аналіз існуючих загроз для ЦВЗ та відповідно методів нанесення ЦВЗ з подальшим дослідженням їх переваг та недоліків.

Виходячи із отриманих результатів аналізу, далі для виконання роботи поставлені такі задачі:

– здійснити вдосконалення обраного методу захисту електронних документів від несанкціонованої модифікації;

– розробити алгоритм роботи програмного засобу на основі вдосконаленого методу;

– здійснити проектування та розробку інтерфейсу користувача, а також

реалізацію програмного засобу;

– здійснити тестування розробки та аналіз отриманих результатів;

– економічно обґрунтувати доцільність впровадження здійсненої розробки на практиці на основі вдосконаленого методу вбудовування ЦВЗ для захисту електронних документів.

Виконання поставлених задач дозволить реалізувати основну мету даної роботи, а саме здійснити підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму.

2 ПІДВИЩЕННЯ СТІЙКОСТІ МЕТОДУ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ НА ОСНОВІ УДОСКОНАЛЕНОГО АЛГОРИТМУ RDH

В даному розділі описано підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH. В роботі надається увага алгоритму оборотного приховування даних на основі гістограмного зміщення із використанням дискретного вейвлет-перетворення та адаптивного шуму. В ході написання розділу обґрунтованого запропоноване удосконалення, наведено алгоритми вбудовування та вилучення даних із стегоконтейнера, описано алгоритм роботи програмної розробки на основі удосконаленого методу, а також здійснено вибір програмних засобів для подальшої практичної реалізації програмного додатку.

2.1 Вдосконалення методу захисту електронних документів

Виходячи із результатів проведеного аналізу, описаного в першому розділі було визначено, що одним із найперспективніших методів на сьогодні, що вбудовує ЦВЗ в електронні документи різних форматів, є метод оборотного приховування даних (RDH, reversible data hiding) [31].

Даний метод використовується для забезпечення цілісності цифрового водяного знаку і контейнера. Його суть полягає в тому, що ЦВЗ являє собою інформацію про частини, які були змінені під час вбудовування, тому під час вилучення даних контейнер можна привести до початкового вигляду. Крім цього, таким методом також перевіряється, чи проводились певні зміни над вихідним контейнером після впровадження ЦВЗ.

На сьогоднішній день запропонованого ряд алгоритмів RDH. Відповідно до стратегій вбудовування, ці алгоритми поділяються на п'ять категорій: різницеве розширення, гістограмне зміщення (HS), розширення помилок прогнозування, упорядкування значень пікселів (PVO) та технологія інтерполяції (IT) [31].

Рисунок 2.1 – Технології алгоритму оборотного приховування даних [31]

В даній роботі дослідимо та здійснимо вдосконалення типу гістограмного оборотного зміщення [32]. Гістограмою з рівнями яскравості в діапазоні $[0, L - 1]$ називається дискретна функція $h(r_1) = n_k$, де r_k – k-ий рівень яскравості, n_k – число пікселів яскравості r_k.

Основна проблема даного типу полягає у значному погіршені якості стегоконтейнера, що призводить до зниження якості захисту (оскільки стають видимими вбудовані ЦВЗ), а також збільшенню візуальної помітності внесених змін.

Відповідно, нормалізована гістограма матиме вигляд:

$$p(r_k) = \frac{n_k}{n}, k = 0,1, \dots, L - 1.$$

$$\sum_{k=0}^{L-1} p(r_k) = 1.$$

Проте, даної нормалізації недостатньо у випадку застосування даного методу для захисту електронних файлів від несанкціонованої модифікації.

Проаналізувавши гістограми досліджуваних електронних файлів було зроблено висновок, що гістограми дуже темних зображень характеризуються тим, що ненульові значення гістограми сконцентровані біля нульових рівнів яскравості, а для дуже світлих зображень навпаки – всі ненульові значення сконцентровані в правій частині гістограми.

Таким чином, доцільно припустити, що найбільш оптимальним варіантом для непомітності вбудовуваного ЦВЗ, підвищення коректності даних оборотного перетворення та зручним для сприйняття людиною буде зображення, у якого гістограма близька до рівномірного розподілу. Тобто для забезпечення непомітності ЦВЗ, відповідності початково вбудованих даних та поліпшення візуальної якості до зображення треба застосувати таке перетворення, щоб гістограма результату містила всі можливі значення яскравості та при цьому в приблизно однаковій кількості.

Відповідно, для коригування обраних пікселів гістограмного зміщення для розподілу вбудовуваних даних застосуємо метод дискретного-вейвлет перетворення із використанням модифікованих коефіцієнтів середньочастотної та високочастотної областей.

Низькочастотна область зображень в запропонованому модифікованому алгоритмі не розглядається, оскільки кожна область контейнера являє собою квадратичну матрицю коефіцієнтів перетворення, а в квадраті низькочастотної області знаходяться значимі елементи спектру дискретного-вейвлет перетворення, зміна яких суттєво збільшить візуальну помітність вбудовування та, відповідно, знижуватиме стійкість захисту.

Щоб ускладнити візуальне сприйняття змін файлу-контейнера під час вбудовування ЦВЗ здійснюється додаткове закриття зображення адаптивним шумом [33].

Отже, виходячи із вказаних вимог, вдосконалений алгоритм на основі дискретного вейвлет-перетворення та використання адаптивного шуму можна представити наступними кроками:

Крок 1. Розбиття зображення на квадратичні матриці із $k-$ коефіцієнтів відповідно до нормалізованої гістограми.

Крок 2. Відповідно до алгоритму, встановлення рівня L_{min} та L_{max} значень допустимих змін.

Крок 3. Обробка $k-$ коефіцієнтів матриць середньочастотних та високочастотних областей зображення.

Крок 4. Вбудовування цифрового водяного знаку у групу обраних $k-$ коефіцієнтів G_k.

Процес вбудовування можна представити наступною формулою:

$$G_k = G_k + M[\alpha A_1 + (1-\alpha)A_0 + MG_k],$$

де $G_k -$ група $k -$ модифікованих коефіцієнтів середньо частотної та високочастотної областей; $M -$ вагова матриця; $\alpha -$ значення вбудовуваного біта; $A_x -$ величина, що становить значення загального перетворення для G_k групи коефіцієнтів.

Крок 5. Накладення адаптивного шуму на зображення за формулою:

$$sh = shStd * rand(x, y),$$

де $shStd$ приймає значення в діапазоні $[0 \dots 1]$, $rand -$ випадкова математична величина з нульовим очікуванням.

Крок 6. Виконання кроків 4 – 5 для всіх бітів вбудовування інформації.

Крок 7. Представлення результуючого зображення – контейнера.

Наведений алгоритм представимо у вигляді схеми на рис. 2.2.

Рисунок 2.2 – Алгоритм вбудовування за вдосконаленим методом

За даним алгоритмом, вбудовування буде здійснюватись у модифіковані коефіцієнти згідно з дискретним вейвлет-перетворенням та подальшим накладанням адаптивного шуму, відповідно гістограма такого файлу буде мати однорідний вигляд, мінімальні візуальні зміни, ЦВЗ буде стійким до різного роду атак.

Таким чином, на основі запропонованого удосконаленого методу далі в роботі буде описано алгоритм вбудовування та вилучення даних із електронних файлів та здійснено розробку алгоритму роботи відповідного програмного засобу.

2.2 Розробка алгоритму вбудовування даних в електронні документи

Електронні документи сьогодні використовуються у будь-яких видах діяльності та передаються різноманітними каналами зв’язку. Відповідно до цього, одним із основних завдань в сфері захисту інформації є захист таких електронних документів від несанкціонованої модифікації, тобто внесення змін у файл сторонніми особами, що призводить до підробки даних, некоректної та недостовірної інформації і т.д.

На практиці, найбільш використовуваними форматами електронних документів є файли pdf та jpeg формату, які і будуть досліджені у даній роботі.

Особливості формату JPEG. Стандарт joint photographic experts group (JPEG) [34] – один із найпопулярніших графічних стандартів стиснення сигналів, який використовують для зберігання і передавання зображень у мережі Інтернет.

Алгоритм стандарту JPEG дає змогу домогтися високого коефіцієнта стиснення, зберігаючи при цьому прийнятну якість сигналу. Для забезпечення захисту інформації застосовуються схеми з приховування даних, які впроваджують цифрові водяні знаки у вихідне зображення, утворюючи «помічений» сигнал.

Даний формат має ряд переваг (рис. 2.3), що зумовлюють його широке застосування у електронному документообороті.

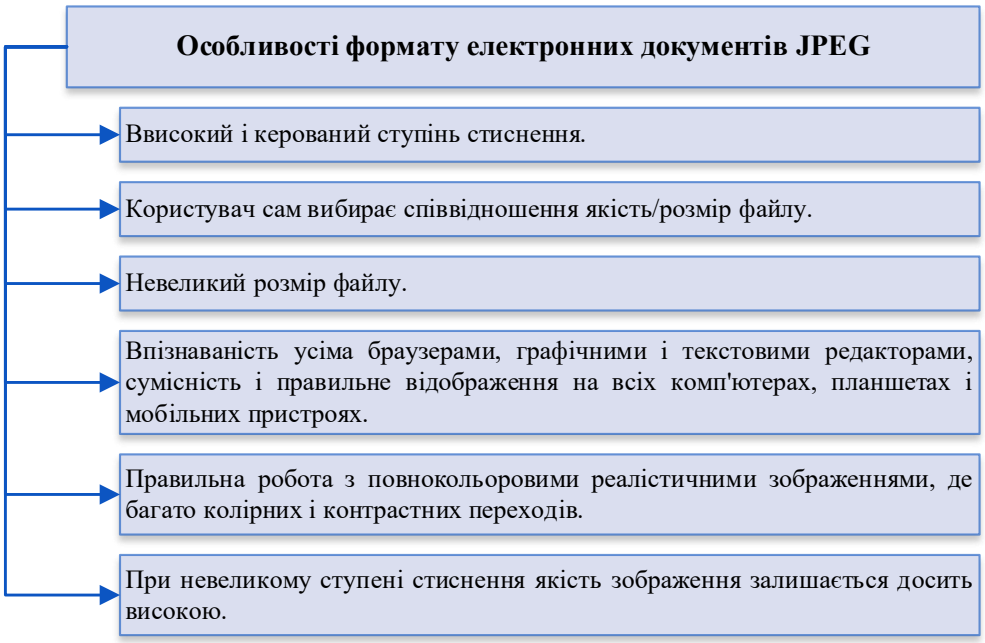


Рисунок 2.3 – Особливості Joint Photographic Experts Group [35]

Далі опишемо алгоритм вбудовування цифрового водяного знаку у растрове зображення на основі вдосконаленого методу із використанням дискретного вейвлет-перетворення [35].

Задамо двовимірний масив B, що має розміри $(2^n + 1) \times (2^n + 1)$, який позначає яскравість конкретної координати за одним із кольорів, де $B[x, y])$ – яскравість пікселя з координатами (x, y) для всіх $x, y = 0 \dots 2^n$.

Далі розглянемо і-й крок: створимо чотири масиви (модель двовимірного wavelet-перетворення):

$$B_i[x, y] = B_{i-1}[2x, 2y]$$

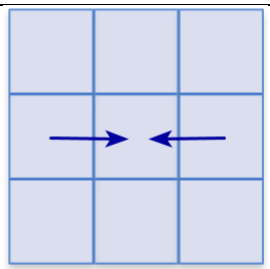
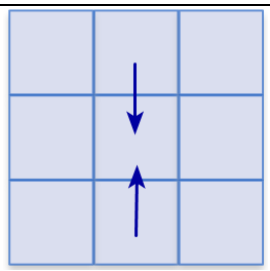
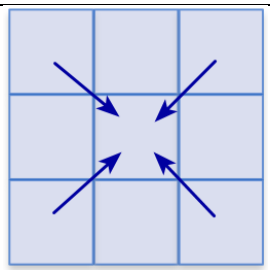
$$H_i\ [x, y] = B_{i-1}[2x + 1{,}2y] - \frac{1}{2}(B_{i-1}[2x, 2y] + B_{i-1}[2x + 2{,}2y]),$$

$$V_i\ [x, y] = B_{i-1}[2x, 2y + 1] - \frac{1}{2}(B_{i-1}[2x, 2y] + B_{i-1}[2x, 2y + 2]),$$

$$C_i\ [x, y] = B_{i-1}[2x + 1{,}2y + 1] - \frac{1}{4}(B_{i-1}[2x, 2y] + B_{i-1}[2x + 2{,}2y] + B_{i-1}[2x, 2y + 2] + B_{i-1}[2x + 2{,}2y + 2]),$$

Для всіх $x, y = 0 \dots 2^{n-1}$.

Таблиця 2.1 – Використовуванні значення

H_i означає відхилення яскравості точки з координатами $(2x+1,2y)$ від середнього арифметичного яскравостей двох сусідніх за горизонталлю точок $(2x,2y)$ і $(2x+2,2y)$	
V_i означає відхилення яскравості точки з координатами $(2x,2y+1)$ від середнього арифметичного яскравостей двох сусідніх за горизонталлю точок $(2x,2y)$ і $(2x,2y+1)$	
C_i означає відхилення яскравості точки з координатами $(2x+1,2y+1)$ від середнього арифметичного яскравостей чотирьох сусідніх точок	

Далі «оновимо» точки масиву B_i:

$$B_i[x,y] = B_i[x,y] + \frac{1}{4}(H_i[x,y] + V_i[x,y] + C_i[x,y]).$$

Оновлення потрібне для того, щоб середня енергія зображення B_i (його середня яскравість) дорівнювала середній яскравості вихідного масиву. Очевидно, що зображення B_{i-1}, і як наслідок, B однозначно відновлюється. Варто також зауважити, що кожного разу, коли обчислюємо нові елементи H_i, V_i, C_i, можна більше не запам'ятовувати ті, що використовували для їхнього обчислення $B_{i-1}[2x+1,2y], B_{i-1}[2x,2y+1], B_{i-1}[2x+1,2y+1]$. Це означає, що алгоритм не залучає додаткової пам'яті. Виконуємо дані кроки до того моменту, поки масив B не буде розміру (2×2).

Тобто, тепер є набори $H_1, V_1, C_1;\ H_2, V_2, C_2;\ \ldots;\ H_n, V_n, C_n$. Варто зауважити, що H_i, V_i, C_i впливають тільки на $2^i + 1$ пікселів, таким чином, кожен крок відповідає різному ступеню різкості (деталізації). Наприклад, для $i = 1$ кожен коефіцієнт впливає на всього лише 3 пікселі, якщо $i = 2$, то на 5 і т. д.

Далі здійснимо вбудовування ЦВЗ у зображення. Для цього потрібно обрати $\alpha \in (0,1)$ – «помітність» (максимальні та мінімальні рівні значень допустимих змін) водяного знака, різкість – крок k і масив H, V або C, на якому і буде введено водяний знак. Нехай для визначеності це буде G_k, тоді замінимо його на масив G'_k такий що:

$$G'_k = G_k + M[\alpha A_1 + (1-\alpha)A_0 + MG_k],$$

Зробимо зворотне вейвлет-перетворення й отримаємо нове зображення.

Особливості формату PDF. Формат PDF (Portable Document Format) є широко використовуваним форматом для представлення електронних документів [36]. Він був розроблений компанією Adobe Systems і є відкритим стандартом ISO 32000-1.

Особливості даного формату наведено на рис. 2.4.

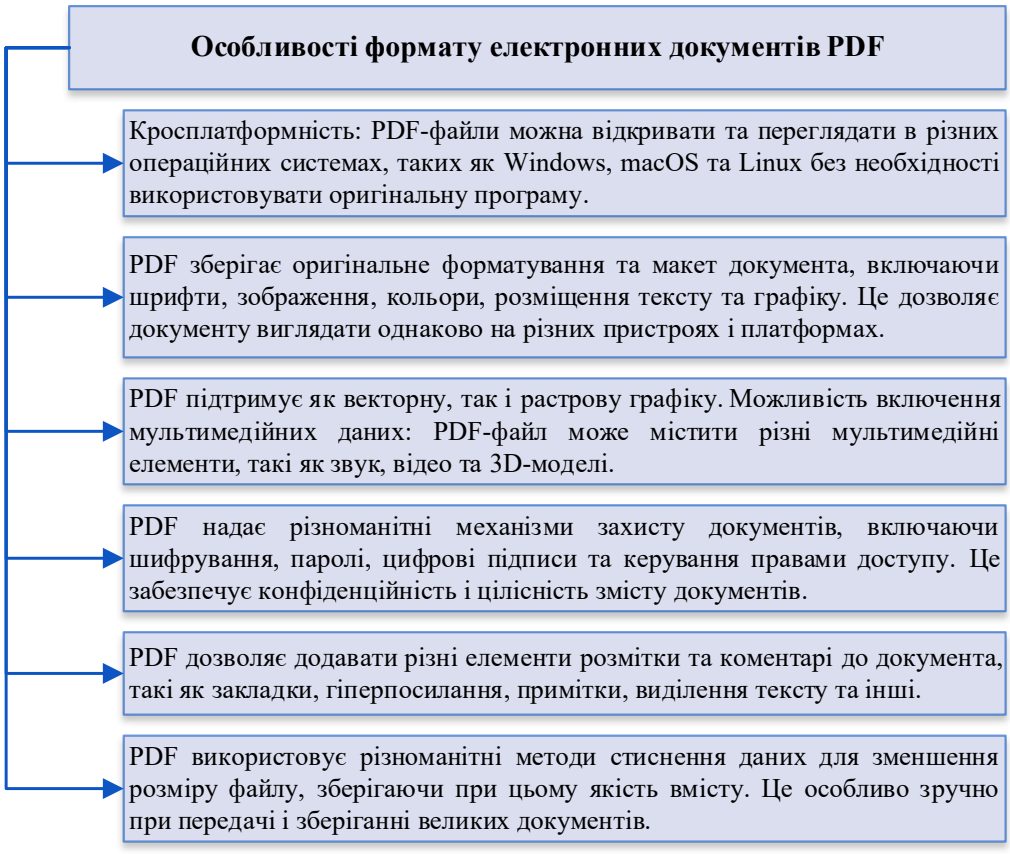


Рисунок 2.4 – Особливості Portable Document Format [37]

Враховуючи особливості даного формату файлів з метою спрощення математичної складності вдосконаленого алгоритму для вбудовування

цифрового водяного знаку здійснимо конвертування сторінок файлу pdf у окремі зображення (які і слугуватимуть стегоконтейнером).

Дане рішення дозволить універсально застосовувати вдосконалений алгоритм, при цьому якість файлу не постраждає, візуальні зміни залишаються непомітними для користувача, а також виконується головне завдання вдосконаленого алгоритму, що полягає у захисті документу від несанкціонованої модифікації.

Для конвертації файлів в роботі запропоновано використати програмну бібліотеку iTextSharp.

Таким чином, враховуючи особливості обраних файлів електронних документів та вдосконаленого алгоритму, далі в роботі здійснимо розробку алгоритму програмного додатку, що має на меті практичну реалізацію методу для вбудовування цифрових водяних знаків у електронні документи з метою їх захисту від несанкціонованої модифікації.

2.3 Розробка алгоритму роботи програмного додатку

На основі вдосконаленого методу захисту електронних документів від несанкціонованої модифікації розробимо програмний додаток, функціоналом якого буде передбачена можливість вбудовування та вилучення цифрового водяного знаку із використанням ключової зашифрованої фрази та можливістю перегляду внесених змін у файл у випадку його модифікації.

Для роботи з програмним додатком користувачеві потрібно мати обліковий запис, захищуваний файл повинен відповідати заданим форматам (pdf, jpeg) та мати відповідні розміри. Загальний алгоритм роботи додатку представимо у вигляді таких кроків:

Крок 1. Запуск програмного додатку.

Крок 2. Авторизація користувача (введення логіну та паролю). У випадку відсутності облікового запису – реєстрація в системі.

Крок 3. Вибір однієї із функцій додатку за допомогою функціональних кнопок.

Крок 4. Введення ключа шифрування (за алгоритмом AES).

Крок 5. Вибір файлу для вбудовування (вилучення) цифрового знаку (ключової фрази).

Крок 6. Перевірка параметрів обраного файлу. Файл повинен мати формат pdf або jpeg та розмір до 300 Мб.

Крок 6.1. У випадку якщо розмір або формат обраного файлу не відповідає встановленим вимогам – користувач отримує відповідне повідомлення.

Крок 6.2. У випадку якщо параметри обраного файлу відповідають вимогам – відбувається перехід до кроку 7.

Крок 7. Перевірка типу файлу.

Крок 7.1. Якщо обрано файл у форматі jpeg – відбувається перехід до кроку 9.

Крок 7.2. Якщо обрано файл у форматі pdf – відбувається перехід до кроку 8.

Крок 8. Конвертація вмісту файлу у файли формату jpeg. Потім – перехід до кроку 9.

Крок 9. Введення ключової фрази (тексту для шифрування), що вбудовуватиметься (вилучатиметься) у якості цифрового водяного знаку у біти файлу.

Крок 10. Підтвердження вбудовування (вилучення) ключової фрази за допомогою відповідної функціональної кнопки.

Крок 10.1 У випадку успішного вбудовування даних у захищуваний файл – відбувається перехід до кроку 11.

Крок 10.2. У випадку якщо виконувалось вилучення даних, користувач отримує ключову фразу (що свідчить про те, що файл не був модифікований), або повідомлення про спробу модифікації захищуваного файлу (навіть, у випадку внесення найменших змін у файл).

Крок 11. Збереження захищеного файлу.

Крок 12. Завершення роботи з програмним додатком.

Схематично даний алгоритм наведено на рис. 2.5.

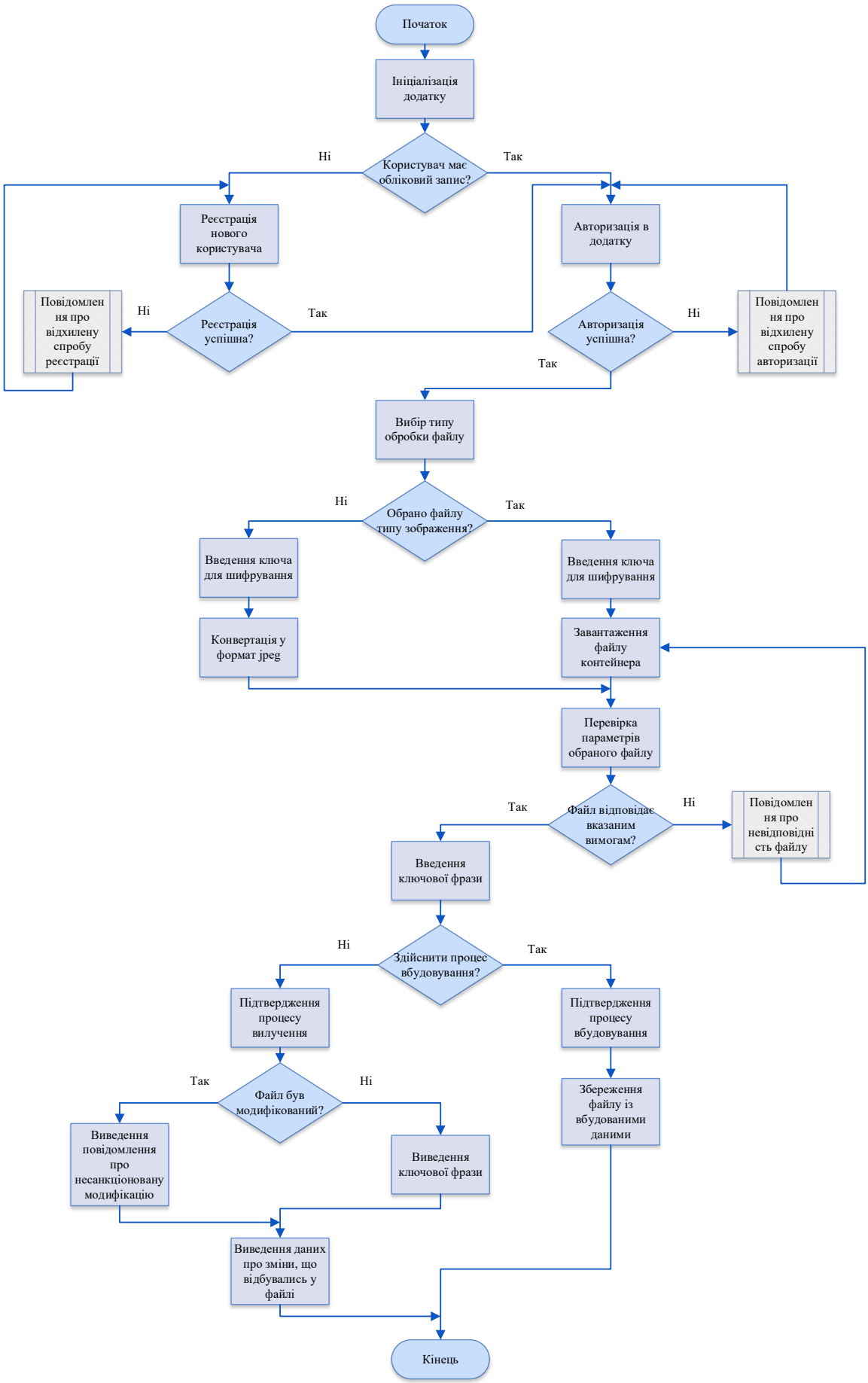


Рисунок 2.5 – Блок-схема алгоритму роботи програмного додатку

Отже, на основі розробленого алгоритму далі в роботі буде реалізовано програмний додаток для захисту електронних документів від несанкціонованої модифікації на основі удосконаленого методу.

Вибір засобів програмування для реалізації даного додатку відповідно до поставлених задач, буде здійснено у наступному підрозділі.

2.4 Обґрунтування вибору засобів програмування

Виходячи із поставлених завдань роботи, для реалізації програмного додатку на основі вдосконаленого стеганографічного методу для захисту електронних документів від несанкціонованої модифікації застосуємо наступні програмні засоби:

– мова об’єктно-орієнтованого програмування C#;

– середовище програмування Visual Studio 2022;

– інтерфейс програмування додатків Windows Forms;

– програмна технологія для створення додатків .NET Framework.

C# – це об'єктно-орієнтована мовою програмування, розроблена компанією Microsoft [37]. Вона є однією з ключових мов для розробки програмного забезпечення на платформі .NET, а також вважається однією з найпопулярніших мов програмування в контексті розробки програмного забезпечення для Windows та веб-програмування.

Основні особливості мови програмування, що зумовили її вибір для даної роботи наведені на рис. 2.6.

Visual Studio є інтегрованим середовищем розробки (IDE – Integrated Development Environment), розробленим компанією Microsoft [38].

Дане середовище надає розробникам засоби і сервіси для створення, відлагодження, тестування та розгортання програмного забезпечення для різних платформ.

Основні особливості середовища розробки, що зумовили його вибір для даної роботи наведені на рис. 2.7.

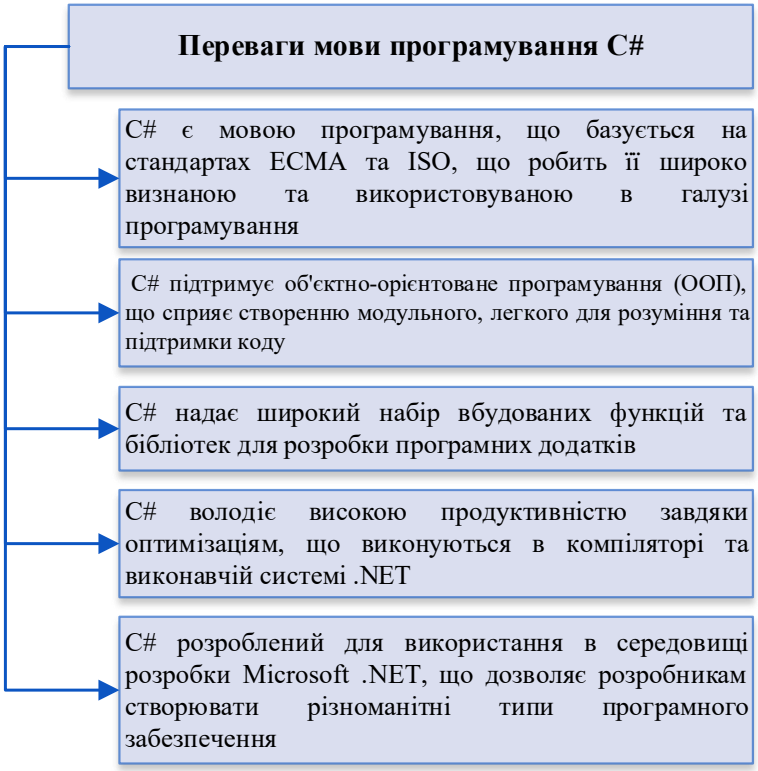


Рисунок 2.6 – Основні переваги обраної мови програмування C# [37]

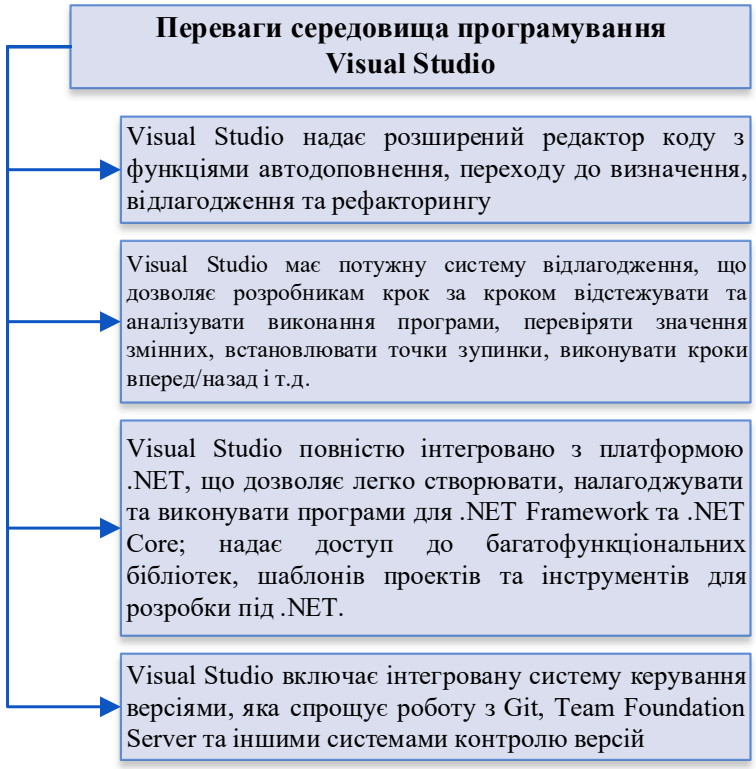


Рисунок 2.7 – Основні переваги обраного середовища програмування Visual Studio [38]

Windows Forms (WinForms) – це набір класів і бібліотек, які входять до складу .NET Framework і використовуються для створення графічних інтерфейсів користувача (GUI) в програмах під управлінням операційної системи Windows [39].

Основні особливості технології, що зумовили її вибір для даної роботи наведені на рис. 2.8.

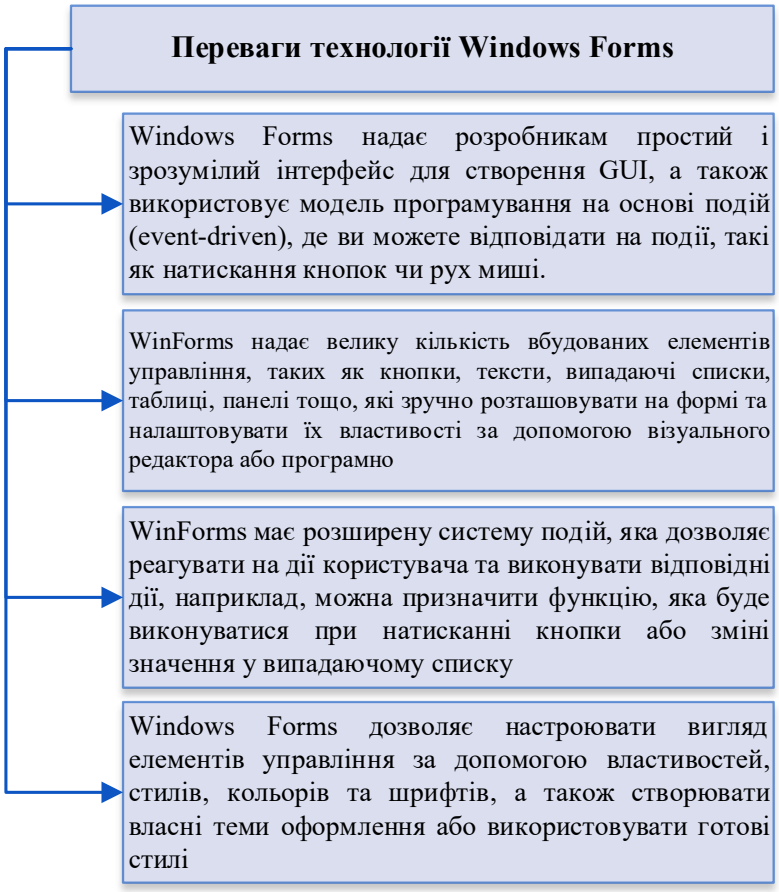


Рисунок 2.8 – Основні переваги обраної технології Windows Forms [39]

Microsoft .NET Framework є програмною платформою, розробленою компанією Microsoft, яка надає середовище для розробки та виконання програмного забезпечення [40].

NET Framework складається з двох основних компонентів:

– Common Language Runtime (CLR) – це загальномовне середовище виконання, у якому функціонують додатки NET;

– Base Class Library (BCL) – набір бібліотек класів .NET Framework. Усі

мови програмування в середовищі NET використовують цю бібліотеку, зокрема, C#.

Основні особливості технології, що зумовили її вибір для даної роботи наведені на рис. 2.9.

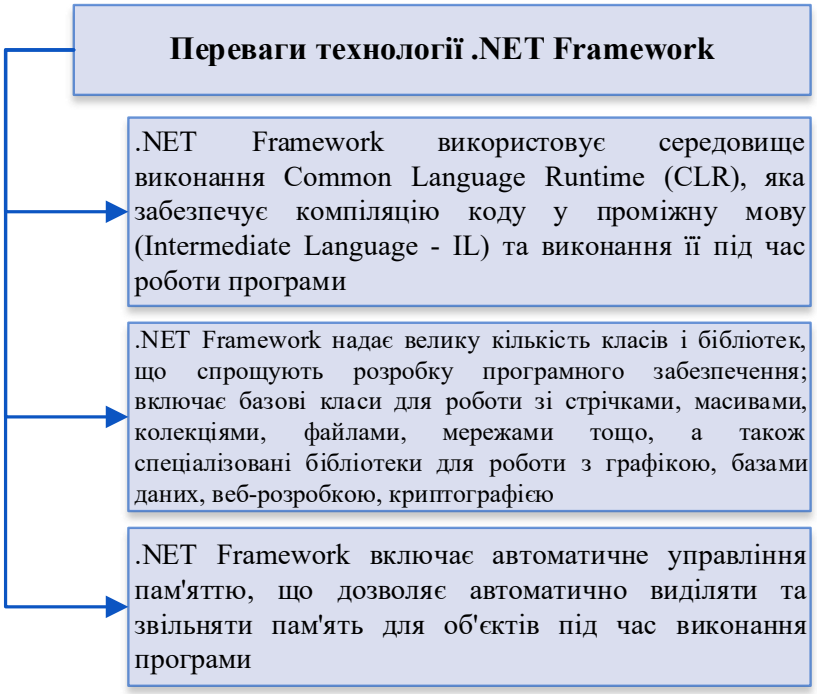


Рисунок 2.9 – Основні переваги обраної технології .NET Framework [40]

Далі в роботі на основі обраних засобів програмування буде здійснено розробку програмного додатку методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

2.5 Висновки до розділу

Отже, в даному розділі було здійснено розробку методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH, а саме його гістограмного типу оборотного зміщення.

Оскільки, основна проблема даного типу полягає у значному погіршені якості стегоконтейнера, що призводить до зниження якості захисту (оскільки

стають видимими вбудовані ЦВЗ і збільшується ймовірність знищення або пошкодження ЦВЗ), а також збільшенню візуальної помітності внесених змін, то відповідно, в якості удосконалення для коригування обраних пікселів гістограмного зміщення для розподілу вбудовуваних даних застосуємо метод дискретного-вейвлет перетворення із використанням модифікованих коефіцієнтів середньочастотної та високочастотної областей.

Низькочастотна область зображень в запропонованому модифікованому алгоритмі не розглядається, оскільки в ній знаходяться значимі елементи спектру дискретного вейвлет-перетворення, зміна яких суттєво збільшить візуальну помітність вбудовування та, відповідно, знижуватиме стійкість захисту. Щоб ускладнити візуальне сприйняття змін файлу-контейнера під час вбудовування ЦВЗ здійснюється додаткове закриття зображення адаптивним шумом.

Виходячи із запропонованого удосконалення, в даному підрозділі була описана його математична модель, здійснена розробка алгоритму вбудовування цифрового водяного знаку у електронні документи формату jpeg та pdf, розробленого алгоритм роботи програмного додатку на основі вдосконаленого методу.

Виходячи із поставлених завдань роботи, для реалізації програмного додатку було обрані програмні засоби: мова програмування C#; середовище програмування Visual Studio 2022; інтерфейс програмування додатків Windows Forms; програмна технологія для створення додатків .NET Framework. Детальний покроковий опис практичної реалізації розробки опишемо у наступному розділі.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ВДОСКОНАЛЕНОГО МЕТОДУ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ

В даному розділі опишемо етапи практичної реалізації програмної розробки, що призначена для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму. В ході написання розділу буде здійснено розробку графічного користувацького інтерфейсу, описано особливості програмної реалізації додатку на основі обраних засобів програмування, таких як C#, Visual Studio 2022, Windows Forms та .NET Framework; наведено інструкцію користувача для роботи з програмою, а також проведено тестування вдосконаленого алгоритму на основі програмної розробки для визначення практичних результатів роботи.

3.1 Розробка графічного інтерфейсу програмної розробки

При розробці будь-якого програмного додатку розробнику слід звернути увагу на користувацький інтерфейс (UI) – візуальну частину розробки, що визначає спосіб взаємодії користувача з програмним додатком, пристроєм чи системою [41]. Користувацький інтерфейс являє собою набір елементів, таких як кнопки, поля введення, меню, панелі, вікна та інші, які дозволяють користувачеві комунікувати з програмою та керувати її функціональністю.

Основними завданнями користувацького інтерфейсу є сприяння виконанню прямих функцій додатку, навігація по додатку, представлення необхідної інформації, забезпечення взаємодії використовуваного програмного забезпечення та користувача [42].

Враховуючи дані особливості, ключовими вимогами до розробки користувацького інтерфейсу є [43]:

– простота та легкість у використанні (користувачеві повинно бути зрозуміло як навігувати по програмі та взаємодіяти з її елементами);

– зрозумілість дизайну (інтерфейс повинен бути логічним, простим у використанні та інтуїтивно зрозумілим для користувача; елементи управління, такі як кнопки, меню, форми, повинні мати зрозумілі та доступні назви та символи);

– ефективність та продуктивність (інтерфейс повинен бути скомпонований максимально лаконічно та зрозуміло шляхом зменшення кількості кроків та розташування необхідних елементів управління в логічній послідовності).

Вимоги та особливості розробки інтерфейсу варіюють залежно від потреб та призначень програмного додатку.

Оскільки, розроблюваний в даній роботі програмний додаток призначений для опрацювання файлів та має практичну цінність виключно у прямому використанні його основного функціоналу, інтерфейс додатку повинен мати стриманий дизайн, зрозумілі функціональні клавіші та лаконічні діалогові форми для взаємодії користувача та програми).

Розглянемо структуру декількох вікон розроблюваного додатку.

Після запуску програми, відкривається її головне вікно. Функціоналом додатку перебачено, що користуватись ним можуть лише авторизовані користувачі.

Тому у верхній частині головного вікна програми розміщено функціональні кнопки «Вхід» та «Реєстрація», в основній частині вікна містяться основні відомості про додаток (наприклад, назва), у нижній частині вікна розташована кнопка «Інструкція», після натиснення на яку відкриватиметься вікно із описом призначення програми. За потреби власника додатку, там можуть бути розміщені контакти, або будь-які інші дані.

Для акаунту авторизованого користувача в даному вікні ще з’явиться кнопка «Працювати з файлами».

Проектований вигляд даного вікна наведено на рис. 3.1.

Наступне діалогове вікно складається з двох функціональних кнопок та призначене для вибору подальшого напрямку роботи користувача: робота із зображеннями у форматі jpeg та робота із файлами у форматі pdf.

Проектований вигляд даного вікна наведено на рис. 3.2.

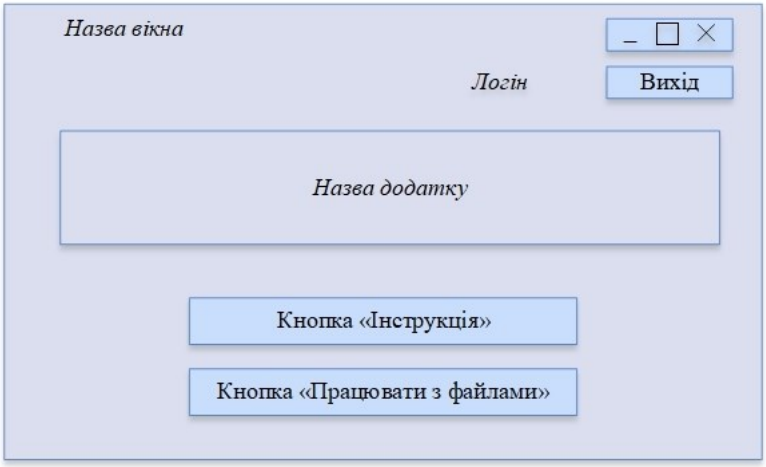


Рисунок 3.1 – Проектування вигляду головного вікна додатку

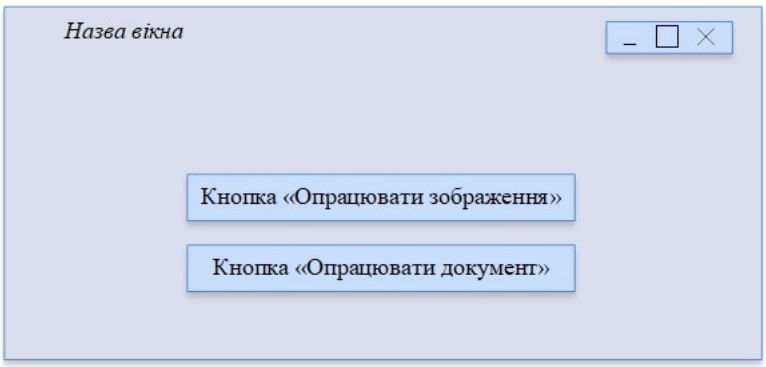


Рисунок 3.2 – Проектування вигляду вікна додатку для вибору типу файлів

Одне із основних вікон програми – це власне вікно, де буде здійснюватись обробка зображення або pdf-документа. У верхній частині даного вікна розташовані поля для відображення обраного користувачем електронного документа.

У випадку, якщо це одне зображення, то буде представлено один графічний елемент. У випадку, якщо це файл pdf, то буде наведено декілька графічних елементів, що відображатимуть сторінки даного документу.

Нижче у вікні буде розташована кнопка «Завантажити» та поле для введення ключової фрази, що шифрується за відповідним алгоритмом та попередньо вказаним ключем. Нижче розташована кнопка «Вбудувати».

У випадку успішного вбудування цифрового водяного знаку, користувачеві відкриється директорія та надасться можливість вказати ім’я файлу та обрати шлях збереження. Вигляд даного вікна наведено на рис. 3.3.

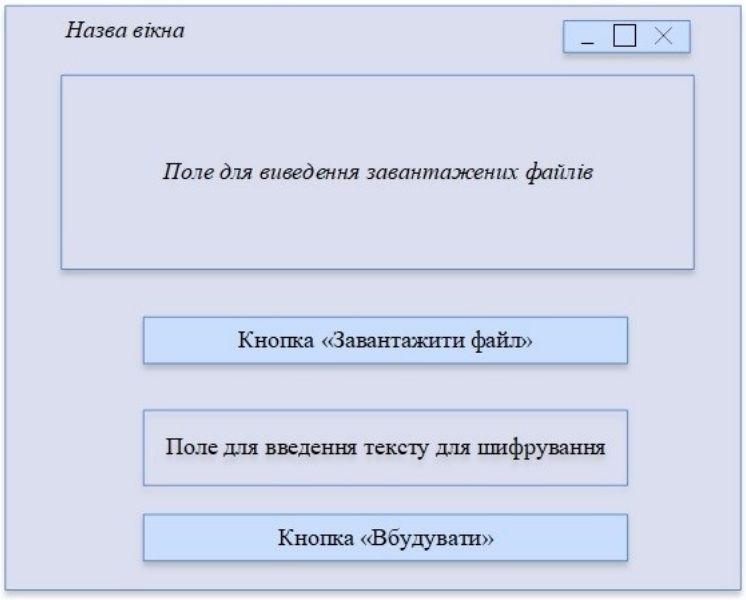


Рисунок 3.3 – Проектування вигляду вікна додатку для обробки файлів

Для наочного представлення результатів внесених змін передбачено ще одне вікно програми (рис. 3.4), що автоматично відкриватиметься після вбудовування ЦВЗ у файли. У такому вікні можна буде переглянути відтворені піксельні зміни здійснені за вдосконаленим алгоритмом та для порівняння із алгоритмом LSB.

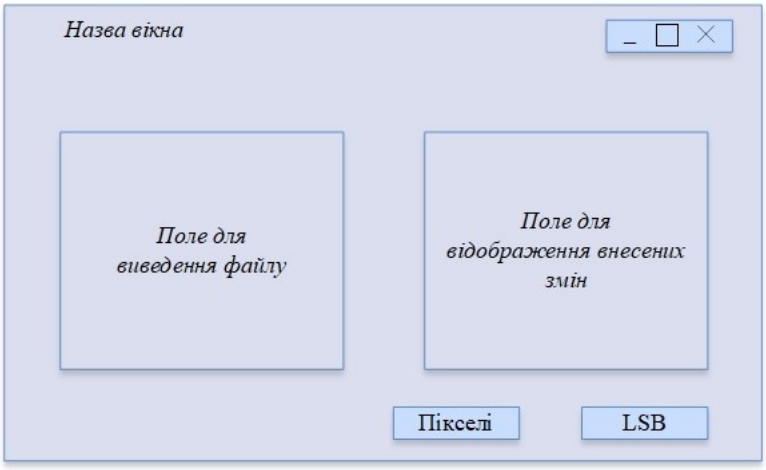


Рисунок 3.4 – Проектування вигляду вікна додатку для відображення змін

Таким чином, на основі спроектованих вікон, далі в роботі буде здійснено розробку програмного інтерфейсу для розроблюваного програмного додатку, що має на меті вбудовування цифрових водяних знаків в електронні документи.

3.2 Програмна реалізація додатку на основі вдосконаленого методу

В даному розділі опишемо основні фрагменти коду, що були реалізовані в роботі з метою розробки програмного додатку для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму.

Для роботи підключені наступні бібліотеки:

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
```

Реалізація форми авторизації та реєстрації:

```
 private void button1_Click(object sender, EventArgs e)
      {
         var users = GetUsers();
         if(users == null)
         {
            MessageBox.Show("Користувача не знайдено");
            return;
         }
         var dbUser = users.FirstOrDefault(x => x.UserName == textBox1.Text && x.Password
== textBox2.Text);
         if (dbUser == null)
         {
            var dbUserLog = users.FirstOrDefault(x => x.UserName == textBox1.Text);
            if (dbUserLog != null)
            {
               MessageBox.Show("Невірний пароль");
               return;
            }
            MessageBox.Show("Користувача не знайдено");
            return;
```

```
            }

            string json1 = JsonConvert.SerializeObject(new User()
            {
               Password = textBox2.Text,
               UserName = textBox1.Text,
            });

File.WriteAllText($"{Path.GetDirectoryName(System.AppDomain.CurrentDomain.BaseDirectory)}/
TempFile.json", json1, Encoding.UTF8);
            this.Hide();
            Home sistema = new Home(true, textBox1.Text);
            sistema.ShowDialog();
            this.Close();
         }
```

Кнопка для вибору функції вбудовування цифрового водяного знаку у файли формату pdf:

```
private void button2_Click(object sender, EventArgs e)

      {
         this.Hide();
         PdfHomePage sistema = new PdfHomePage();
         sistema.ShowDialog();
         this.Close();
      }
```

Кнопка для вибору функції вбудовування цифрового водяного знаку у файли формату jpeg:

```
 private void button1_Click(object sender, EventArgs e)
      {
         this.Hide();
         ImageHomePage sistema = new ImageHomePage();
         sistema.ShowDialog();
         this.Close();
      }
```

Обробка файлів формату jpeg:

```
Bitmap bmp = new Bitmap(pictureBox1.Image);
         for (int i = 0; i < bmp.Width; i++)
         {
            if (i % 10 == 0)
            {
               for (int j = 0; j < bmp.Height; j++)
               {
                  Color cc = bmp.GetPixel(i, j);
```

```
                listBox1.Items.Add("R:" + cc.R.ToString() + "G:" + cc.G.ToString() + "B:" +
cc.B.ToString());

            }
        }
    }
```

Програмна реалізація вдосконаленого алгоритму для вбудовування цифрового водяного знаку та фіксації модифікації:

```
public static Bitmap embedText(string text, Bitmap bmp)
    {
        State s = State.hiding;
        int charIndex = 0;
        int charValue = 0;
        long colorUnitIndex = 0;
        int zeros = 0;
        int R = 0, G = 0, B = 0;
        for (int i = 0; i < bmp.Height; i++)
        {
            for (int j = 0; j < bmp.Width; j++)
            {
                Color pixel = bmp.GetPixel(j, i);
                pixel = Color.FromArgb(pixel.R - pixel.R % 2,
                    pixel.G - pixel.G % 2, pixel.B - pixel.B % 2);
                R = pixel.R; G = pixel.G; B = pixel.B;
                for (int n = 0; n < 3; n++)
                {
                    if (colorUnitIndex % 8 == 0)
                    {
                        if (zeros == 8)
                        {
                            if ((colorUnitIndex - 1) % 3 < 2)
                            {
                                bmp.SetPixel(j, i, Color.FromArgb(R, G, B));
                            }
                            return bmp;
                        }
                        if (charIndex >= text.Length)
                        {
                            s = State.filling_with_zeros;
                        }
                        else
                        {
                            charValue = text[charIndex++];
                        }
                    }
                    switch (colorUnitIndex % 3)
                    {
```

```
                    case 0:
                        {
                            if (s == State.hiding)
                            {
                                R += charValue % 2;

                                charValue /= 2;
                            }
                        }
                        break;
                    case 1:
                        {
                            if (s == State.hiding)
                            {
                                G += charValue % 2;

                                charValue /= 2;
                            }
                        }
                        break;
                    case 2:
                        {
                            if (s == State.hiding)
                            {
                                B += charValue % 2;

                                charValue /= 2;
                            }
                            bmp.SetPixel(j, i, Color.FromArgb(R, G, B));
                        }
                        break;
                }
                colorUnitIndex++;

                if (s == State.filling_with_zeros)
                {
                    zeros++;
                }
            }
        }
    }
    return bmp;
}
```

Програмна реалізація вдосконаленого алгоритму для вилучення цифрового водяного знаку та фіксації модифікації:

```
public static string extractText(Bitmap bmp)
    {
```

```
        int colorUnitIndex = 0;
        int charValue = 0;
        string extractedText = String.Empty;
        for (int i = 0; i < bmp.Height; i++)
        {
            for (int j = 0; j < bmp.Width; j++)
            {
                Color pixel = bmp.GetPixel(j, i);
                for (int n = 0; n < 3; n++)
                {
                    switch (colorUnitIndex % 3)
                    {
                        case 0:
                            {
                                charValue = charValue * 2 + pixel.R % 2;
                            }
                            break;
                        case 1:
                            {
                                charValue = charValue * 2 + pixel.G % 2;
                            }
                            break;
                        case 2:
                            {
                                charValue = charValue * 2 + pixel.B % 2;
                            }
                            break;
                    }
                    colorUnitIndex++;
                    if (colorUnitIndex % 8 == 0)
                    {
                        charValue = reverseBits(charValue);

                        if (charValue == 0)
                        {
                            return extractedText;
                        }

                        char c = (char)charValue;
                        extractedText += c.ToString();
                    }
                }
            }
        }
        return extractedText;
    }
```

Шифрування даних ключової фрази за криптографічним алгоритмом AES для додаткового захисту вмісту ЦВЗ:

```
public static string DecryptStringAES(string cipherText, string sharedSecret)
    {
      if (string.IsNullOrEmpty(cipherText))
        throw new ArgumentNullException("cipherText");
      if (string.IsNullOrEmpty(sharedSecret))
        throw new ArgumentNullException("sharedSecret");
      RijndaelManaged aesAlg = null;
      string plaintext = null;
      try
      {
        Rfc2898DeriveBytes key = new Rfc2898DeriveBytes(sharedSecret, _salt);
        byte[] bytes = Convert.FromBase64String(cipherText);
        using (MemoryStream msDecrypt = new MemoryStream(bytes))
        {
          aesAlg = new RijndaelManaged();
          aesAlg.Key = key.GetBytes(aesAlg.KeySize / 8);
          aesAlg.IV = ReadByteArray(msDecrypt);
          ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key, aesAlg.IV);
          using (CryptoStream csDecrypt = new CryptoStream(msDecrypt, decryptor,
CryptoStreamMode.Read))
          {
            using (StreamReader srDecrypt = new StreamReader(csDecrypt))
              plaintext = srDecrypt.ReadToEnd();
          }
        }
      }
      finally
      {
        if (aesAlg != null)
          aesAlg.Clear();
      }
      return plaintext;
    }
```

Обробка даних при здійсненні процесу вилучення ключових даних із стегоконтейнера, зокрема перевірка ключової фрази, ключа для розпізнавання ключової фрази, а також перевірка чи здійснювалась модифікація файлу:

```
private void button2_Click_1(object sender, EventArgs e)
    {
      Bitmap bmp = (Bitmap)pictureBox1.Image;
      string extractedText = SteganographyHelper.extractText(bmp);
      var s = extractedText.Split(':');
      if (s.Length < 2 || s[0] != Key)
      {
        MessageBox.Show(@"Невірний ключ");
        return;
      }
```

```
            if (!s[1].StartsWith("value"))
            {
              MessageBox.Show(@"Ключова фраза не розпізнана. Файл зазнав модифікації.");
              return;
            }
            var val = s[1].Replace("value", "");
            textBox1.Text = val;
          }
```

Отже, в даному підрозділі наведено ключові кодові фрагменти, що були описані для практичної програмної реалізації розроблюваного додатку на основі вдосконаленого методу.

Лістинг програмної розробки наведений у додатках Б та В даної роботи.

3.3 Інструкція користувача для роботи з програмним додатком

Для роботи з додатком користувачеві необхідно здійснити запуск виконуваного файлу. Після його відкриття буде доступне діалогове вікно, що містить загальну інформацію про додаток (рис. 3.5).

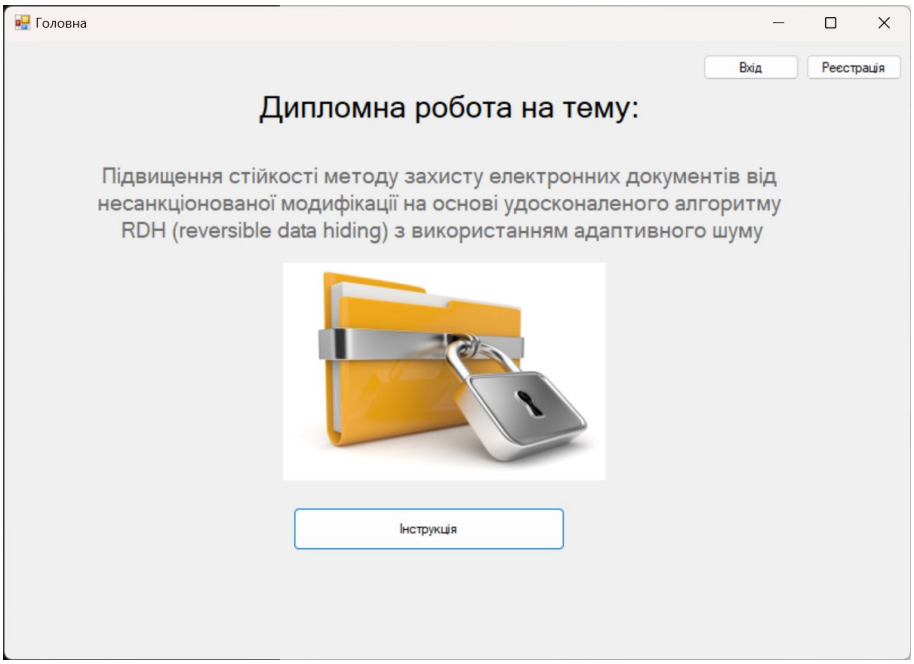


Рисунок 3.5 – Вигляд головного вікна додатку

Також у головному вікні програми для неавторизованого користувача доступна кнопка «Інструкція», при натисненні на яку відкривається вікно із описом функціоналу програмної розробки (рис. 3.6).

За необхідності, при практичному впроваджені можуть бути додані кнопки «Контакти» та будь-які інші дані передбачені поставленими задачами.

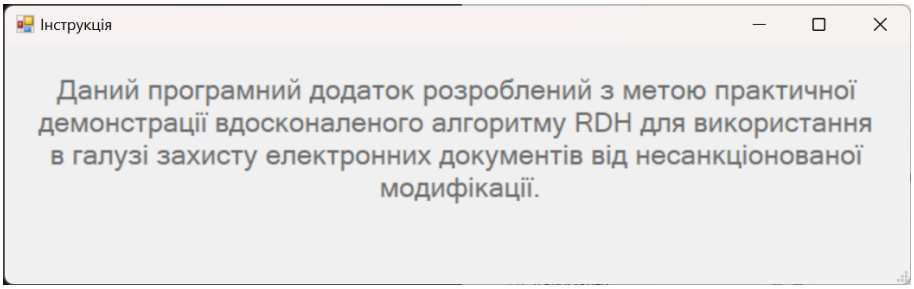


Рисунок 3.6 – Вигляд вікна з додатковою інформацією

Для продовження роботи з додатком користувачеві слід здійснити вхід в систему, скориставшись кнопками «Вхід» або «Реєстрація», у випадку, якщо облікового запису у користувача немає. При практичному впроваджені розробки дані для авторизації можуть бути змінені на будь-які інші форми залежно від потреб.

У демонстраційній версії розроблюваного додатку для авторизації в системі достатньо ввести логін та пароль (рис. 3.7).

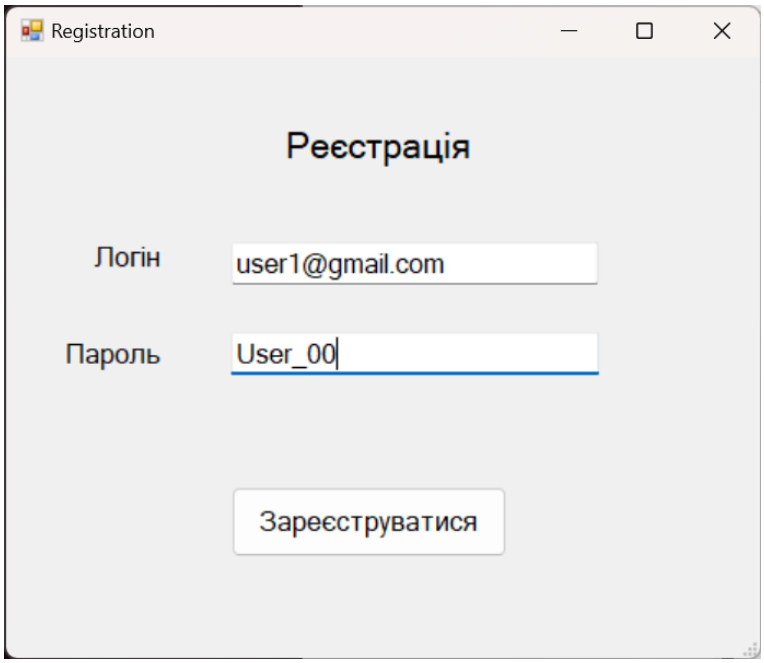


Рисунок 3.7 – Вигляд вікна реєстрації користувача

У випадку, якщо під час процесу авторизації користувач вводить невірний пароль або логін, або при реєстрації користувач із вказаним логіном уже

зареєстрований – видається відповідне сповіщення (рис. 3.8).

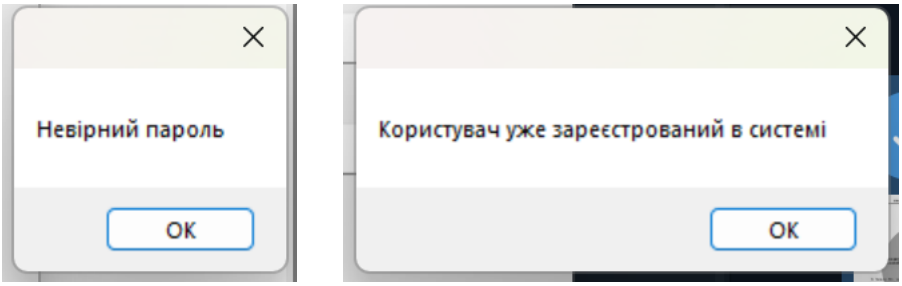


Рисунок 3.8 – Сповіщення при невдалих спробах авторизації

Далі, для авторизованих в системі користувачів на головному вікні додатку з’являється функціональна кнопка для початку роботи з файлами, а у правому верхньому куті відображається логін користувача (рис.3.9).

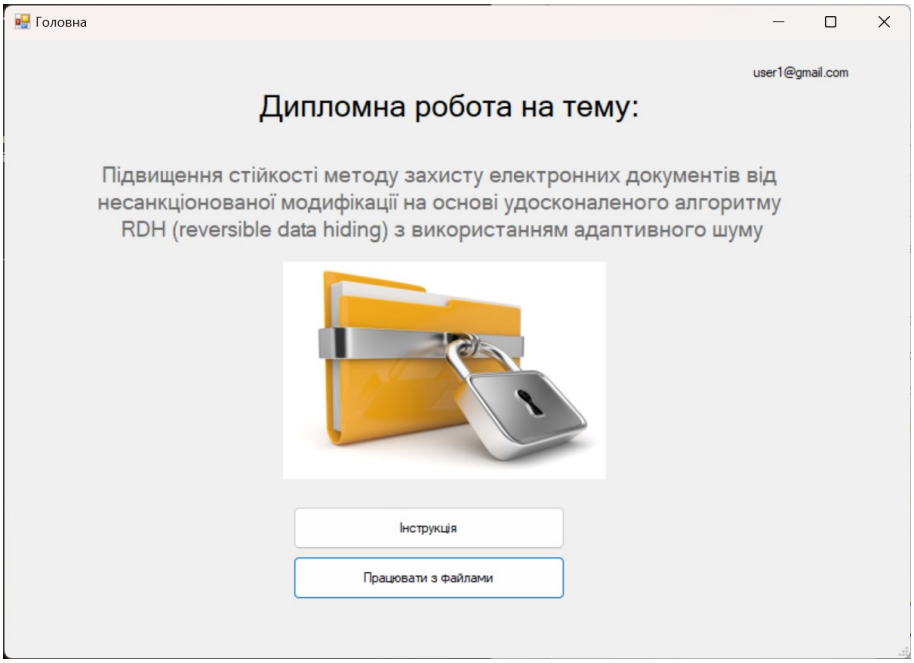


Рисунок 3.9 – Вигляд головного вікна додатку авторизованого користувача

Після натиснення кнопки працювати з файлами відривається наступне діалогове вікно, яке передбачає вибір користувачем формату файлів для подальшої роботи (рис. 3.10).

В межах даної роботи обрані формати електронних документів такі як jpeg та pdf.

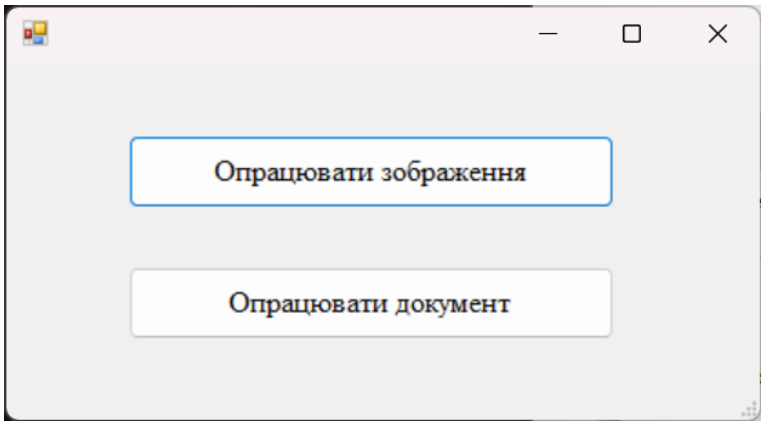


Рисунок 3.10 – Вигляд вікна для вибору формату файлу для подальшої роботи

Спочатку для прикладу розглянемо процес вбудовування цифрового водяного знаку у файли формату jpeg. Після натиснення кнопки «Опрацювати зображення» відкривається наступне діалогове вікно, де користувач повинен ввести відкритий ключ, що буде застосовуватись для шифрування ключової фрази та обрати відповідну функцію «Вбудовування» або «Вилучення» даних із зображення (рис. 3.11).

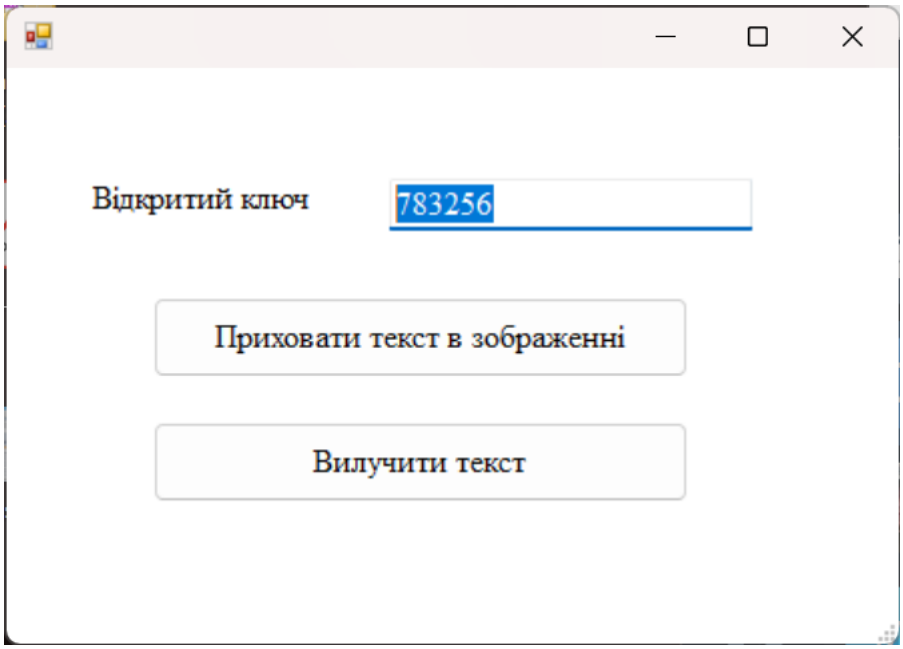


Рисунок 3.11 – Вигляд вікна для вибору відповідної функції

В наступному діалоговому вікні користувачеві необхідно завантажити відповідне зображення, ввести ключову фразу, що являтиме собою невидимий цифровий водяний знак та буде попередньо зашифрована (рис. 3.12).

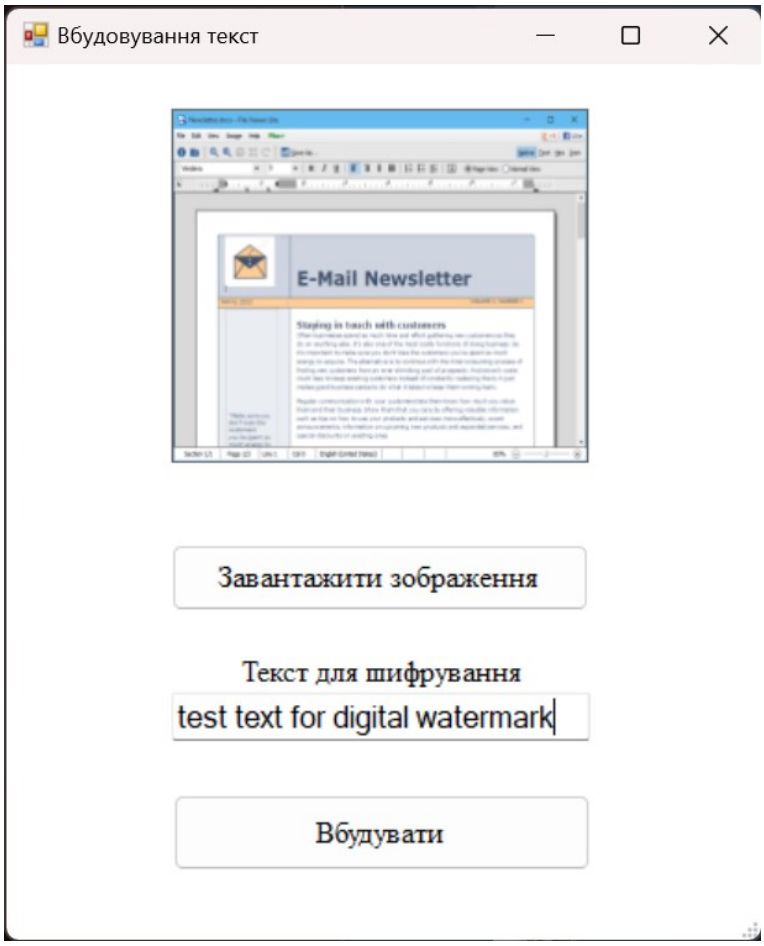


Рисунок 3.12 – Вигляд вікна для опрацювання файлу

Після натиснення кнопки «Вбудувати» в результаті успішного вбудовування цифрового водяного знаку, відкривається директорія і користувач може задати ім’я створеного файлу та зберегти його у потрібній теці.

Після виконання вказаної дії – автоматично відкривається наступне діалогове вікно програмного додатку, що відображає внесені у файл зміни (рис. 3.13).

Натиснувши кнопку «Пікселі» користувач зможе переглянути які частини файлу були задіяні для вбудовування цифрового водяного знаку та будуть застосовані для збереження даних про модифікацію.

Для прикладу, поряд також розташована кнопка «LSB», натиснувши на яку, можна побачити яких змін зазнає файл, у випадку вбудовування даних за методом найменш значущого біта (рис.3.14).

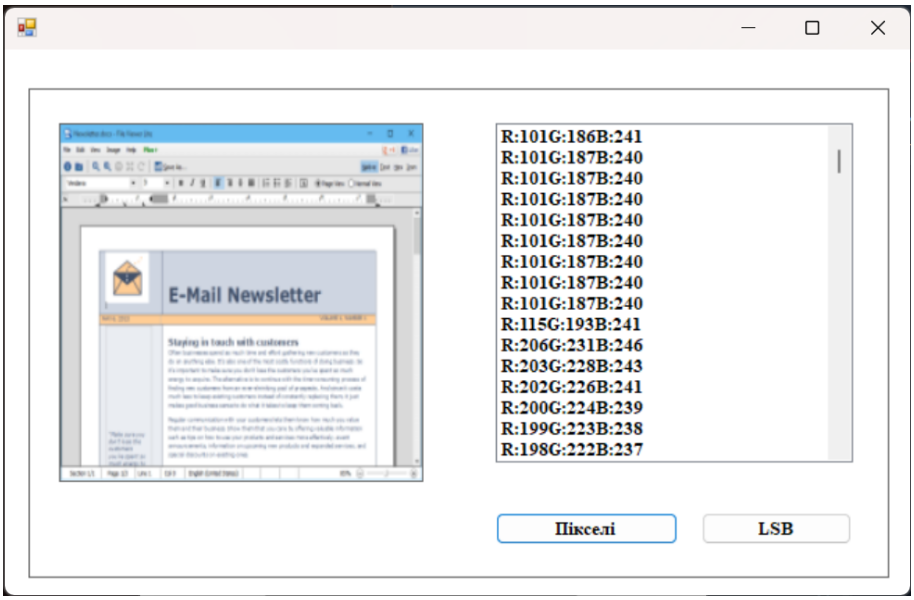


Рисунок 3.13 – Вигляд вікна із відображенням внесених змін за вдосконаленим алгоритмом

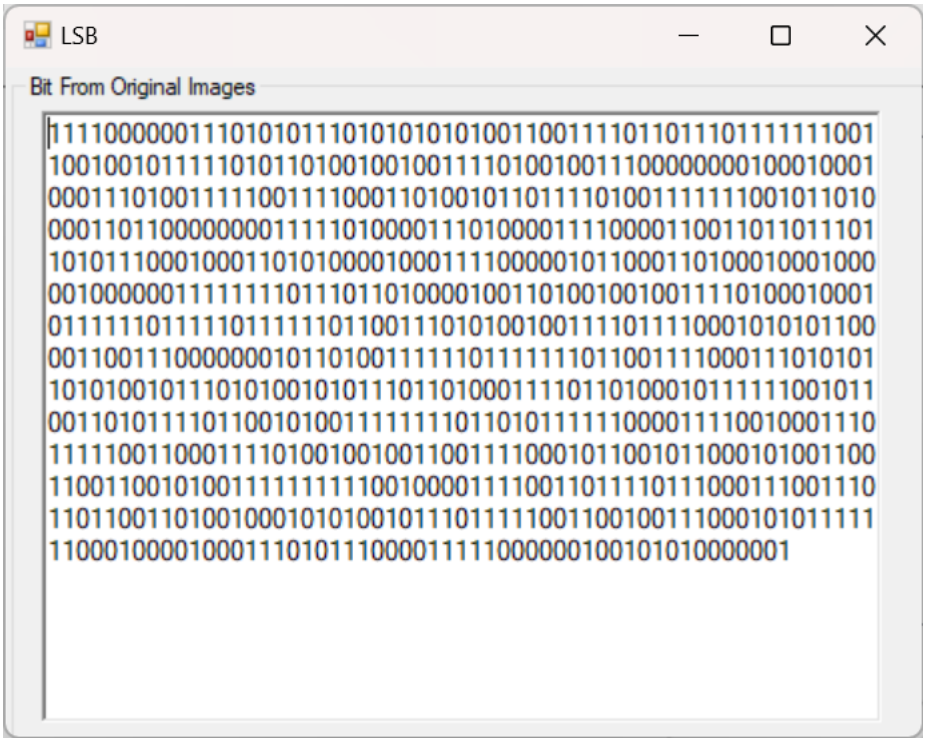


Рисунок 3.14 – Вигляд вікна, що відображає внесенні зміни за алгоритмом LSB

Для вилучення даних із стегоконтейнера у вікні (рис. 3.11) користувачеві слід ввести ключ, що був використаний при вбудовуванні ЦВЗ та скористатись кнопкою «Вилучити дані». У вікні, що буде після цього відкрито (рис. 3.15), користувачеві слід вибрати відповідний файл стегоконтейнер та натиснути

кнопку «Вилучити».

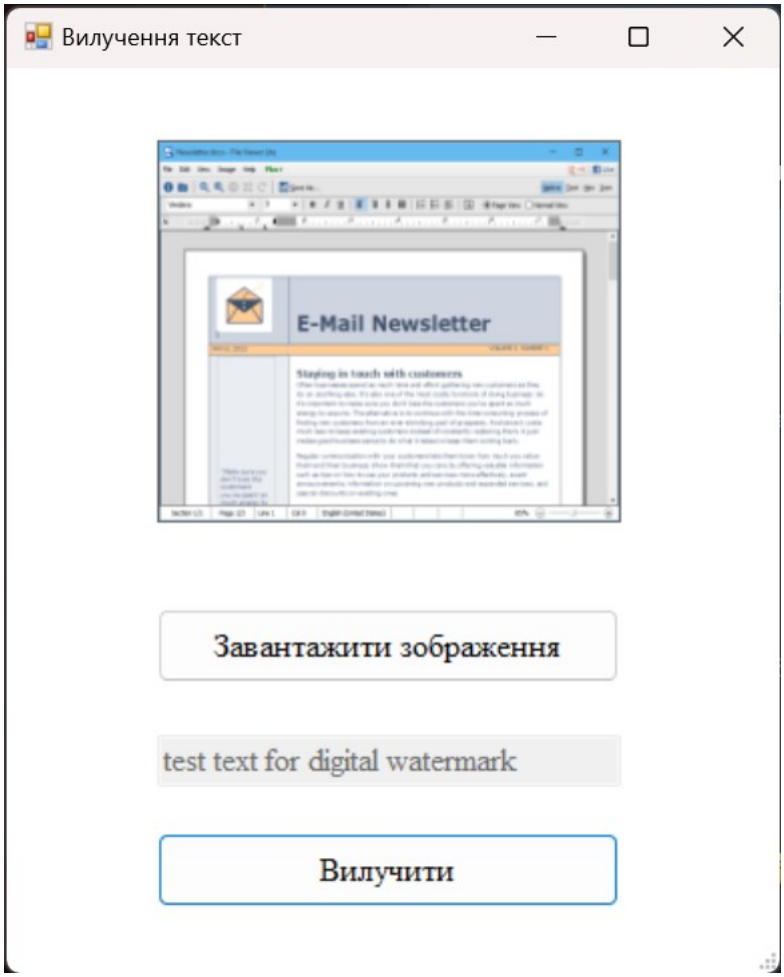


Рисунок 3.15 – Вигляд вікна для вилучення даних із зображення

Якщо всі дані коректні і файл не зазнавав модифікації, у відповідному полі буде виведена ключова фраза, що була застосована для цифрового водяного знаку (як це показано на рис. 3.15). У випадку, якщо користувач застосував некоректний ключ, буде отримано відповідне сповіщення (рис. 3.16).

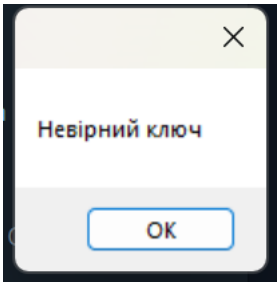


Рисунок 3.16 – Сповіщення про некоректний ключ для опрацювання файлу

У випадку, якщо оброблюваний файл зазнав змін, ключова фраза не буде розпізнана коректно, а користувач отримає сповіщення про те, що файл зазнав модифікації (рис. 3.17).

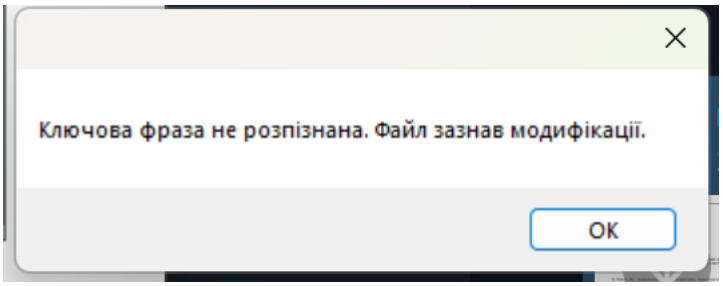


Рисунок 3.17 – Сповіщення про спробу модифікації файлу

Для обробки файлів формату pdf застосовується аналогічний процес, відмінність якого полягає у додатковому алгоритмі для конвертації формату pdf у формат jpeg. Дана функція дозволяє зробити удосконалений метод універсальним та придатним до застосування більшості файлів, при цьому не втрачається якість вбудовування цифрового водяного знаку, якість самого файлу для типопового користувача та не знижується ступінь захисту від модифікації.

Вигляд вікна завантаженого для опрацювання файлу pdf наведено на рис. 3.18.

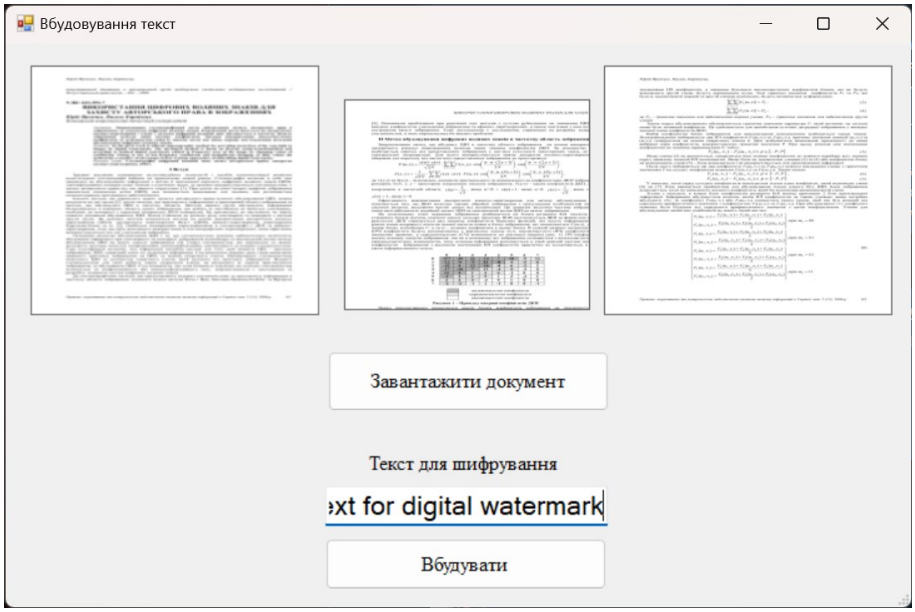


Рисунок 3.18 – Вигляд вікна із завантаженим файлом для опрацювання

Після вбудовування цифрового водяного знаку та збереження результуючого файлу, аналогічним чином можна переглянути внесені зміни (рис. 3.19 і рис. 3.20).

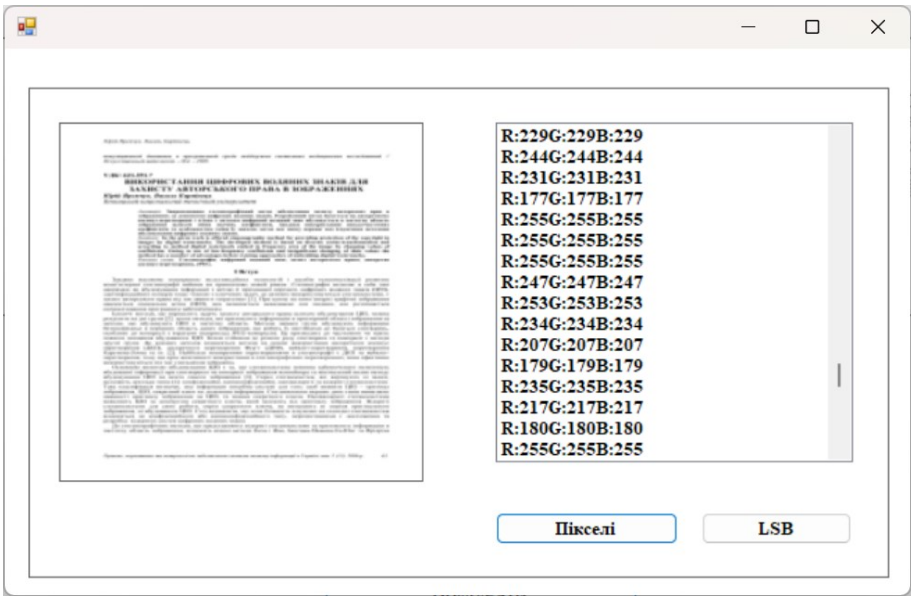


Рисунок 3.19 – Вигляд вікна із відображенням внесених змін за вдосконаленим алгоритмом

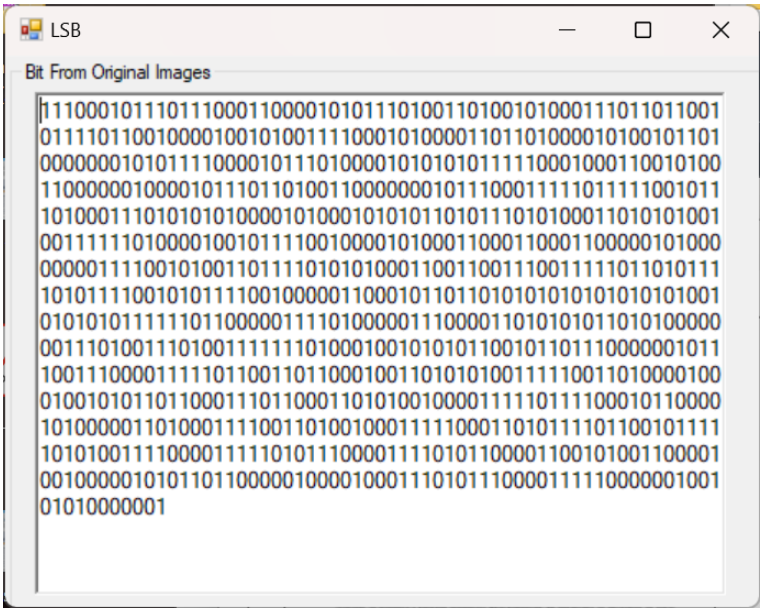


Рисунок 3.20 – Вигляд вікна, що відображає внесенні зміни за алгоритмом LSB

При успішному вилучені даних із опрацьованого файлу – відображається вбудовування у цифровий водяний знак ключова фраза (рис. 3.21).

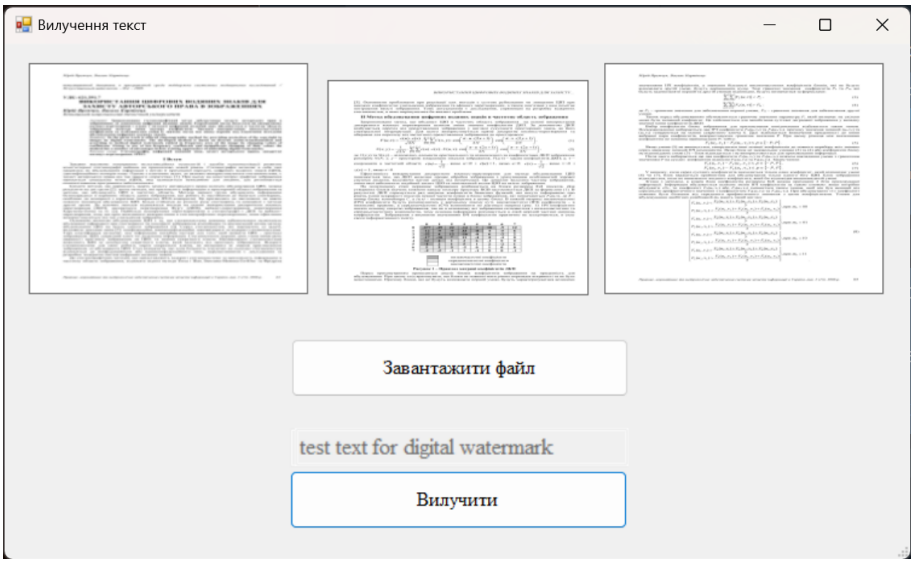


Рисунок 3.21 – Вигляд вікна для вилучення даних із зображення

У випадку якщо відкритий ключ некоректний або файл зазнав модифікації, користувачеві виводяться відповідні сповіщення (рис. 3.16 і рис. 3.17).

Таким чином, у даному підрозділі на прикладі практичного застосування було описано інструкцію для роботи користувача з додатком, основна функція якого полягає у практичній реалізації вдосконаленого методу з метою захисту електроних документів від несанкціонованої модифікації.

3.4 Аналіз тестування програмного додатку на основі вдосконаленого методу

В даній роботі проводилось дослідження та практична розробка програмного додатку для захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH. З метою визначення практичної доцільності та раціональності здійсненого вдосконалення проведемо тестування реалізованого додатку на предмет стійкості до різного роду атак, форматування та захисту від модифікації.

Першим етапом тестування, дослідимо стійкість методу до спотворення рівномірним шумом (додавання до значень кожного пікселя зображення в кожному із каналів червоного, зеленого та синього кольорів (RGB) випадкової величини в інтервалі від N до N, де N – рівень шуму).

Для проведення дослідження було використано вдосконалений алгоритм, а також аналоги розглянуті в першому розділі (табл. 3.1). Для тестування аналогів було використано додатковий програмний додаток (код у відкритому доступі).

Таблиця 3.1 – Стійкість методів до спотворення рівномірним шумом

Метод	Рівень рівномірного шуму								
	10	20	30	40	50	65	75	85	100
Вдосконалений метод	0	0	0	0	0	0	0,01	0,1	0,16
Гістограмний метод	0	0	0	0	0,01	0,12	0,13	0,19	0,22
Метод випадкових інтервалів	0	0	0	0	0	0,06	0,1	0,23	0,33
Метод блокового приховування	0	0	0	0,05	0,1	0,15	0,18	0,2	0,23

Максимально можливий рівень шуму, що призводить до втрати вихідного зображення становить 255, проте отримані результати тестування свідчать про те, що спотворення зображення спостерігаються при рівні 75). І даний показник належить саме вдосконаленому методу.

Дані результати тестування свідчать про те, що вдосконалений метод має більшу стійкість порівняно зі своїми аналогами, а також методу, відносно якого відбувалось вдосконалення.

Наступним кроком тестування визначимо стійкість алгоритмів до jpeg-стиснення.

Для проведення дослідження стиснемо зображення за алгоритмом jpeg з різними значеннями параметра, що відповідає за якість стиснення (табл. 3.2).

Таблиця 3.2 – Стійкість методів до jpeg-стиснення

Метод	Коефіцієнт якості jpeg-стиснення								
	100	85	75	60	50	40	30	20	10
Вдосконалений метод	0	0	0	0	0,03	0,1	0,25	0,37	0,42
Гістограмний метод	0	0	0	0,05	0,11	0,21	0,28	0,43	0,51
Метод випадкових інтервалів	0	0	0	0,06	0,14	0,19	0,26	0,37	0,45
Метод блокового приховування	0	0,01	0,06	0,1	0,13	0,2	0,32	0,41	0,53

За результатами тестування найбільшу стійкість до даного типу спотворення має вдосконалений алгоритм, а також близький до нього метод випадкових інтервалів.

Варто зауважити, що показники стійкості вдосконаленого методу суттєво вищі від показників методу відносно якого здійснювалось удосконалення.

Здійснимо тестування вдосконаленого алгоритму за показниками, що найчастіше використовуються на практиці, зокрема:

– максимальне співвідношення сигнал / шум ($PSNR$):

$$PSNR = XY \cdot \frac{max_{x,y\,(C_{x,y})^2}}{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2}$$

– середня абсолютна відмінність (AD):

$$AD = \frac{1}{XY}\sum_{x,y}|C_{x,y} - S_{x,y}|$$

– структурна подібність ($SSIM$):

$$SSIM\,(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + x_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)}$$

Для тестування було обрано десять зразків електронних документів, що містили у собі цифровий водяний знак у вигляді текстової фрази «test text for

digital watermark» (розмір кожного символу 8 біт, загальний розмір фрази 248 біт). Протестовано вдосконалений метод, гістограмний метод, метод випадкових інтервалів, метод блокового приховування.

Результати тестування наведемо у вигляді діаграми (рис. 3.22, рис. 3.23, рис. 3.24).

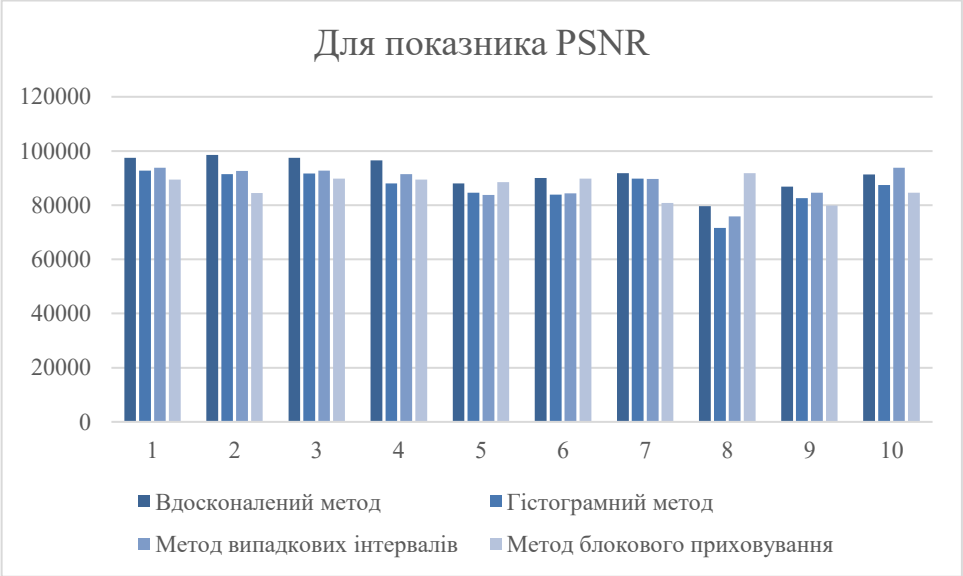


Рисунок 3.22 – Результати тестування за показником $PSNR$

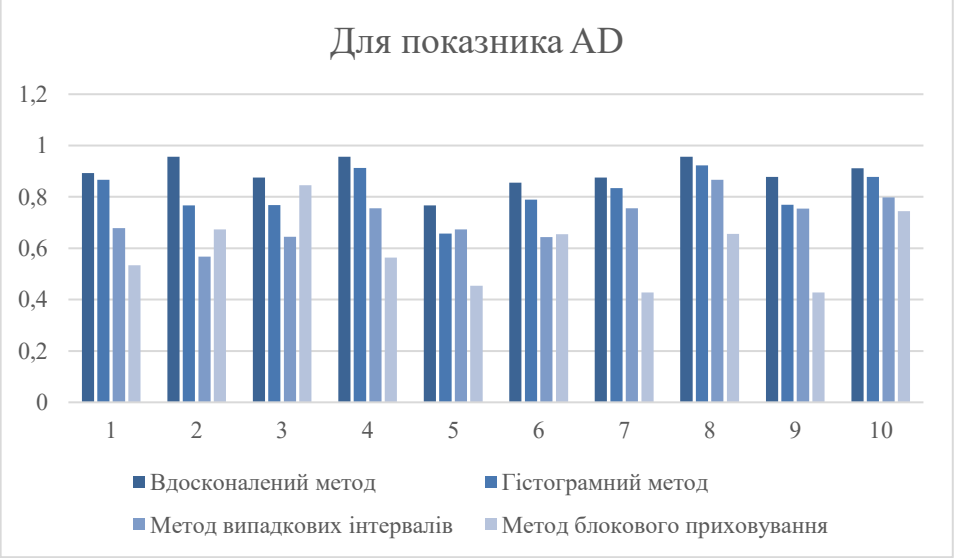


Рисунок 3.23 – Результати тестування за показником AD

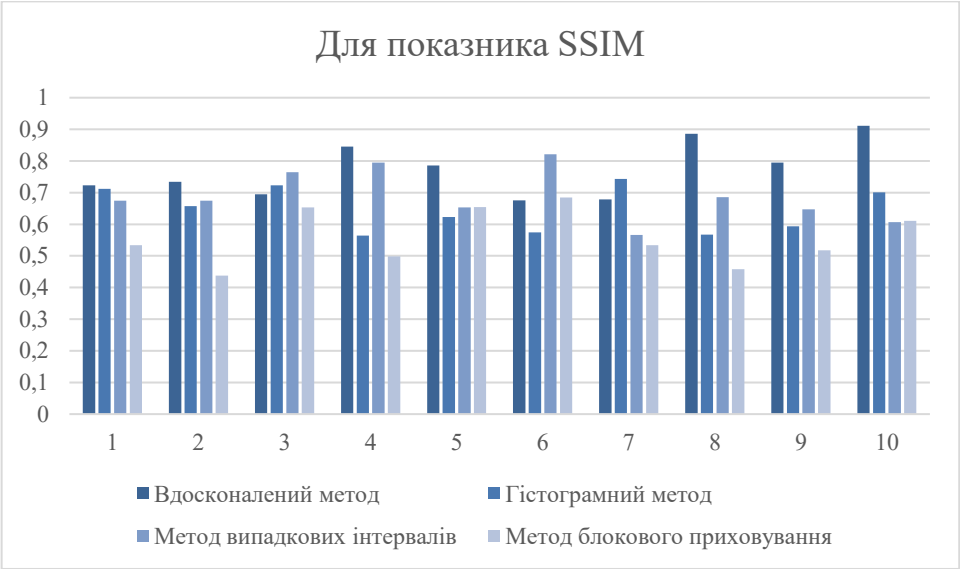


Рисунок 3.24 – Результати тестування за показником $SSIM$

Як можна побачити із наведених діаграм, вдосконалений метод має високі кількісні показники, що свідчить про успішне тестування та якісну реалізацію.

Оскільки, основним завданням роботи є захист електронних документів від модифікації, важливо, щоб цифровий водяний знак, який зберігає дані про модифікацію був робастним, тобто стійким до змін контейнера несанкціонованими користувачами.

У зв’язку з цим, дослідимо стійкість стеганоконтейнера до обрізання файлу, поворотів (віддзеркалень), зміни яскравості, а також надання чорно-білого відтінку, згладжування медіанним фільтром.

Для проведення дослідження відберемо п’ятдесят зразків (100%) та визначимо відсоток робастних ЦВЗ вбудовуваних різними методами, зокрема, вдосконаленим методом на основі RDH, гістограмним методом, методом випадкових інтервалів, методом блокового приховування.

У таблиці 3.3 наведемо у відсотках кількість ЦВЗ, що були стійкими до вказаних змін та повністю зберегли інформацію, що містилась у ЦВЗ.

Таблиця 3.3 – Відсоткове співвідношення робастних ЦВЗ до вказаних змін

Метод	Обрізання файлу	Повороти / віддзеркалення	Зміна яскравості	Надання чорно-білого відтінку	Згладжування медіаним фільтром
Вдосконалений метод	92%	95%	97%	96%	93%
Гістограмний метод	85%	88%	91%	90%	83%
Метод випадкових інтервалів	84%	85%	93%	87%	82%
Метод блокового приховування	82%	81%	89%	85%	82%

Наведенні результати тестування свідчать про те, що вбудовані за вдосконаленим методом цифрові водяні знаки стійкі до поширених впливів на контейнер, а результат вдосконалення свідчить про підвищення стійкості методу порівняно з основним орієнтовно на 7%.

Далі на рисунках 3.25, 3.26 та 3.27 представимо оригінальне зображення (зліва) та дане зображення із вбудованим ЦВЗ (справа) для демонстрації візуальних змін зображення внаслідок вбудовування за вдосконаленим методом.

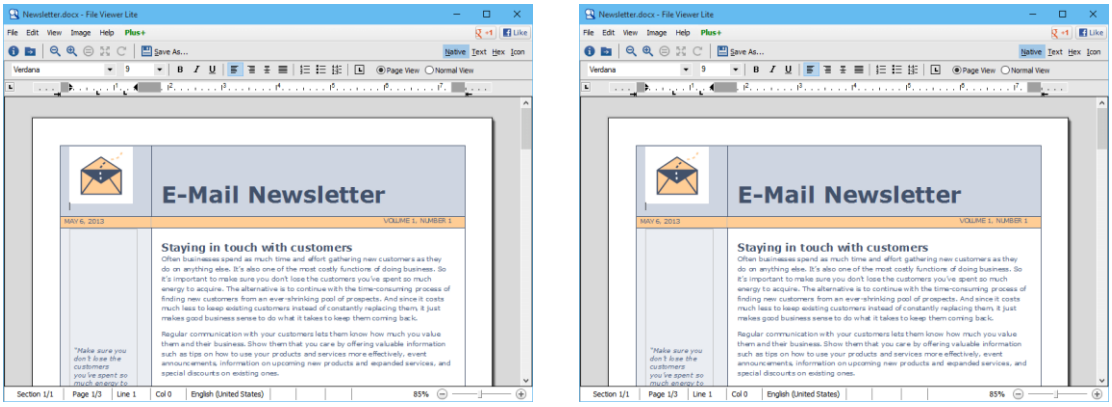


Рисунок 3.25 – Зразок оригінального зображення та стегоконтейнера (дослід 1)

Рисунок 3.26 – Зразок оригінального зображення та стегоконтейнера (дослід 2)

Рисунок 3.27 – Зразок оригінального зображення та стегоконтейнера (дослід 3)

Як можна побачити з наведених зразків, незалежно від типу зображення (текстове, повнокольорове чи у чорно-білих відтінках) – для людського зору непомітні зміни між оригіналом та стегоконтейнером, що свідчить про ефективність реалізованого методу та коректність застосованого адаптивного шуму.

Таким чином, отримані результати тестування свідчать про успішність вдосконаленого методу та доцільність його застосування на практиці. Вдосконалений метод на основі гістограмного типу має вищі якісні та кількісні показники порівняно з початковим методом, а стійкість алгоритму до впливів на стегоконтейнер підвищена орієнтовно на 7%.

3.5 Висновки до розділу

Отже, у даному розділі на основі обраних засобів програмування таких як C#, Visual Studio 2022, Windows Forms та .NET Framework було здійснено програмну реалізацію додатку для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму.

В ході написання розділу було здійснено розробку графічного користувацького інтерфейсу програмного додатку із врахуванням особливостей розробки; наведено основні фрагменти коду, що були написані для реалізації основного функціоналу розробки. В наступному підрозділі роботи на практичному прикладі було описано інструкцію користувача для роботи з програмою із покроковим описом.

Окремою частиною розділу є аналіз результатів тестування реалізованого програмного додатку на основі вдосконаленого методу з метою визначення практичної доцільності здійснення такого вдосконалення.

Отримані результати тестування свідчать про успішність вдосконаленого методу та доцільність його застосування на практиці. Вдосконалений метод на основі дискретного вейвлет-перетворення має вищі якісні та кількісні показники порівняно з початковим методом, а стійкість алгоритму до впливів на стегоконтейнер підвищена орієнтовно на 7%.

Крім того, здійснено тестування програмного додатку, яке показало, що програма коректно працює на усіх версіях ОС Windows та може бути застосована на практиці в комерційних цілях.

4 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є проведення дослідження економічного потенціалу розробки, зокрема, оцінювання комерційного потенціалу; прогнозування витрат на виконання наукової роботи та впровадження її результатів; прогнозування комерційних ефектів від реалізації результатів розробки та розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Результати даного дослідження уможливлюють прийняття рішення про економічну доцільність розробки програмного засобу з використанням методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму.

4.1 Оцінювання комерційного потенціалу розробки програмного забезпечення

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності [50].

Результатом магістерської кваліфікаційної роботи є розробка програмного засобу з використанням алгоритму для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

Для проведення технологічного аудиту залучено трьох незалежних експертів.

– У межах даної роботи такими експертами є викладачі кафедри МБІС: Грицак А. В. (доц., викл. каф. МБІС ВНТУ); Салієва О.В. (д.ф., викл. каф. МБІС ВНТУ); Карпінець В. В. (к.т.н., доцент каф. МБІС ВНТУ).

Оцінювання комерційного потенціалу буде здійснено за критеріями, що наведені в таблиці 4.1

Таблиця 4.1 – Критерії оцінювання комерційного потенціалу розробки бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Крите-р.	0	1	2	3	4
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатацій ні витрати значно вищі, ніж в аналогів	Експлуатацій ні витрати дещо вищі, ніж в аналогів	Експлуатацій ні витрати на рівні експл. витрат аналогів	Експлуатацій ні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Продовження таблиці 4.1

Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навч. наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої к-ті дозвільних документів на вир-во та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу експертами розробки зведено в таблицю 4.2.

Таблиця 4.2 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали, посада експерта		
	1 – Грицак А.В.	2 – Салієва О.В.	3 – Карпінець В.В.
1	3	3	3
Ринкові переваги (недоліки):			
2	4	2	2
3	3	4	4
4	4	3	3
5	4	3	4
Ринкові перспективи			
6	3	3	3
7	3	3	3
Практична здійсненність			
8	4	4	4
9	4	4	4
10	4	4	4
11	4	4	4
12	4	4	4
Сума балів	$СБ_1 = 43$	$СБ_1 = 41$	$СБ_1 = 42$
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = 42$		

За даними таблиці 4.2 можна зробити висновок, щодо рівня комерційного потенціалу розробки. Врахуємо на результат й порівняємо його з рівнями комерційного потенціалу розробки, що представлено в таблиці 4.3.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

Рівень комерційного потенціалу розробки, становить 42 бали, що відповідає рівню «високий».

Наступним кроком здійснимо аналіз технічної задачі та дослідимо аналоги. Наукова новизна розробки полягає в підвищенні стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

Розробка програмного засобу має на меті практичну реалізацію удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

Розроблюваний програмний продукт у вигляді десктнопного додатку надаватиме можливість користувачам накладати цифровий водяний знак на електронні документи з метою їх захисту від несанкціонованої модифікації.

Виходячи із отриманих результатів дослідження розробленого програмного продукту на основі вдосконаленого алгоритму, можна вважати, що розроблений захист для електронних документів є стійким до багатьох видів атак, вбудований цифровий знак на впливає на якість роботи з файлами та не є помітним для користувачів.

Такі результати досягнуто за рахунок здійсненого в роботі удосконалення алгоритму, а саме внесення змін до математичного апарату алгоритму RDH та використання адаптивного шуму.

Враховуючи виявлені переваги розробленого методу, порівняємо його з аналогами. У таблиці 4.4 наведені основні технічні показники аналога і нового програмного продукту.

Таблиця 4.4 – Основні технічні показники аналога і нового програмного продукту

Показники, %	Аналог	Нова розробка	Відношення параметрів нової розробки до параметрів аналога
Функціональність	85	100	1,2
Надійність	90	100	1,1
Сумісність	75	100	1,3
Супровід	70	100	1,4
Економія ресурсів і часу	75	100	1,3
Простота використання	80	100	1,25

Порівняно з аналогами, розроблений програмний додаток, є універсальним засобом для вбудовування цифрових водяних знаків у електронні документи, стійкість якого перевірена на практиці.

Нове технічне рішення, яке пропонується для розробки, матиме високі показники, порівняно з аналогами та більшою мірою задовольнить потреби споживачів. Тому його розробка та впровадження є актуальним та доцільним.

Програмна розробка на основі обраного та вдосконаленого алгоритму сьогодні є актуальною для використання як для звичайних так і корпоративних користувачів.

Для розповсюдження розробки можуть бути використанні торгові та рекламні майданчики інтернет-магазинів з продажу програмного забезпечення та/або офіційний сайт додатку із встановленою середньою ціною на продукт.

Оскільки, на сьогодні питання захисту електронних документів є актуальними, а технології ЦВЗ успішно використовуються для вирішення таких завдань – цілком ймовірний високий попит на запропонований програмний продукт.

4.2 Прогнозування витрат на виконання наукової роботи та впровадження її результатів

Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи складається з таких етапів:

1-й етап: розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи;

2-й етап: розрахунок загальних витрат на виконання даної роботи;

3-й етап: прогнозування загальних витрат на виконання та впровадження результатів даної роботи.

Виконаємо розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи, за такими статтями та формулами, приймаючи до уваги те, що для розробки інформаційної технології було залучено одного розробника програмного забезпечення.

1. Основна заробітна $З_о$:

$$З_о = \frac{М}{Т_р} \cdot t, \text{грн.} \quad (4.1)$$

де М – місячний посадовий оклад – 35 000 грн.;

$Т_р$ – число робочих днів в місяці; приблизно $Т_р = 20$ днів;

t – число робочих днів для всієї роботи – 45 днів.

Таким чином:

$$З_о = \frac{35\,000}{20} \cdot 45 = 78\,750 \text{ (грн.)}$$

Таблиця 4.5 – Витрати по заробітній платі

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату
Розробник	35 000	1 750	45	78 750
Всього				78 750

2. Додаткова заробітна плата $З_д$ працівників розраховується як 12% від основної заробітної плати:

$$З_д = 0{,}12 \cdot 78\,750 = 9\,450 \text{ (грн.)} - \text{для розробника}$$

3. Нарахування на заробітну плату $Н_{зп}$ розробника становить:

$$Н_{зп} = (З_о + З_д) \cdot \frac{\beta}{100} \quad (4.2)$$

де $З_о$ – основна заробітна плата розробника;

$З_д$ – додаткова заробітна плата розробника;

β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування – 22%.

$$Н_{зп} = (78\,750 + 9\,450) \cdot 0{,}22 = 19\,404 \text{ (грн.)}$$

4. Амортизація обладнання, комп'ютерів та приміщень, які використовувались під час виконання даного етапу роботи розраховуємо за формулою:

$$А = \frac{Ц \cdot Т}{12 \cdot Т_В} \quad (4.3)$$

де Ц – загальна балансова вартість обладнання, приміщення тощо, грн.;

Т – фактична тривалість використання, міс;

$Т_В$ – термін використання обладнання, приміщень тощо, роки.

Розробка програмного забезпечення ведеться орієнтовно 2 місяці.

Для офісного приміщення $А = \frac{85\,000 \cdot 2}{12 \cdot 10} = 2\,703 грн.$; для комп'ютера $А = \frac{25\,000 \cdot 2}{12 \cdot 2} = 2\,083 грн.$; для монітора $А = \frac{12\,000 \cdot 2}{12 \cdot 4} = 1000 грн.$

Розрахунки зведено до таблиці 4.6:

Таблиця 4.6 – Амортизаційні відрахування

Найменування	Балансова вартість (грн.)	Термін використання (років)	Фактична тривалість в-ня, (міс.)	Величина ам.. відрахувань, (грн..)
Офісне приміщення	85 000	10	2	1 417
Комп'ютер	25 000	2	2	2 083
Монітор	12 000	4	2	1 000
			Всього	4 500

5. Витрати на комплектуючі К, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$К = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i \ (грн.) \quad (4.4)$$

де $Н_i$ – кількість комплектуючих *i*-го виду, шт.;

$Ц_i$– ціна комплектуючих *i*-го виду, грн.;

$К_i$ – коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15);

n – кількість видів комплектуючих.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектувальних	Кількість	Ціна за штуку, грн.	Сума, грн.	Примітка
Клавіатура	1	850 грн.	850 грн.	
Комп'ютерна мишка	1	550 грн.	550 грн.	
Всього:			$К_і = 1,2$	1 400 грн.

6. Витрати на силову електроенергію $В_е$ розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п \text{ (грн.)} \quad (4.5)$$

де В – вартість 1 кВт-год. (для підприємців вартість 3,45грн./кВт-год. станом на 01.04.2023р.);

П – установлена потужність обладнання – 0,8 кВт;

Ф – фактична кількість годин роботи обладнання – 360 год. (45 днів по 8 годин);

$К_п$ – коефіцієнт використання потужності.

$$В_е = 3,45 \cdot 0,8 \cdot 360 \cdot 0,14 = 140 \text{ (грн)}.$$

7. Інші витрати $В_{ін}$ охоплюють:

– витрати на управління організацією;

– оплату службових відряджень;

– витрати на утримання, ремонт та експлуатацію основних засобів;

– витрати на опалення, освітлення, водопостачання, охорону праці тощо.

Інші витрати $В_{ін}$ можна прийняти як 100% від суми основної заробітної плати розробника:

$$В_{ін} = 78\,750 \cdot 1 = 78\,750 \text{ (грн)}$$

Послуги Інтернету – 350 грн., канцтовари – 500 грн. Загальна вартість становить:

$$350 + 50 = 850 \text{ (грн.)}$$

8. Сума всіх попередніх статей витрат дає витрати на виконання даної частини роботи – В.

$$В = 78\,750 + 9\,450 + 19\,404 + 4\,500 + 1400 + 140 + 78\,750 + 850$$
$$= 193\,244\ (\text{грн.})$$

9. Проведемо прогнозування загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи. Прогнозування здійснюється за формулою:

$$ЗВ = \frac{В_{заг}}{\beta}, \text{грн.} \quad (4.6)$$

де β – коефіцієнт, який характеризує етап (стадію) виконання даної роботи.

Так, якщо розробка знаходиться:

– на стадії науково-дослідних робіт, то $\beta \approx 0{,}1$;

– на стадії технічного проектування, то $\beta \approx 0{,}2$;

– на стадії розробки конструкторської документації, то $\beta \approx 0{,}3$;

– на стадії розробки технологій, то $\beta \approx 0{,}4$;

– на стадії розробки дослідного зразка, то $\beta \approx 0{,}5$;

– на стадії розробки промислового зразка, $\beta \approx 0{,}7$;

– на стадії впровадження, то $\beta \approx 0{,}9$.

$В_{заг}$ – загальна вартість всієї наукової роботи.

$$В = 193\,244\ (\text{грн.})$$

$$ЗВ = \frac{193\,244}{0{,}7} = 276\,062{,}8\ (\text{грн.})$$

Отже, прогноз загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи складає $276\,062{,}8$ (грн.)

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки

У даному підрозділі проведемо кількісне прогнозування, яку вигоду можна отримати у майбутньому від впровадження результатів виконаної наукової роботи.

В умовах ринку узагальнюючим позитивним результатом, що його

отримує підприємство від впровадження результатів тієї чи іншої розробки, є збільшення чистого прибутку підприємства. Зростання чистого прибутку можна оцінити у теперішній вартості грошей.

Зростання чистого прибутку забезпечить інвестору надходження додаткових коштів, які дозволять покращити фінансові результати діяльності.

Виконання даної наукової роботи та впровадження її результатів складає приблизно 1 рік. Позитивні результати від впровадження розробки очікуються вже в перші місяці після впровадження.

Проведемо детальне прогнозування позитивних результатів та кількісне їх оцінювання по роках.

Обчислимо збільшення чистого прибутку підприємства $\Delta П_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, розраховується за формулою:

$$\Delta П_i = \sum_{1}^{n} (\Delta П_я \cdot N + П_я \cdot \Delta N)_i \qquad (4.7)$$

де $\Delta П_я$ – покращення основного якісного показника від впровадження результатів розробки у даному році;

N – основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукової розробки;

ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки;

$П_я$ – основний якісний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки.

Припустимо, що внаслідок впровадження результатів наукової розробки чистий прибуток підприємства збільшиться на 250 грн., а кількість одиниць (наданих прав на користування сервісом) реалізованої послуги збільшиться:

– протягом першого року – на 500 од.,

– протягом другого року – ще на 800 од.,

– протягом третього року – ще на 900 од.

Орієнтовно: реалізація продукції до впровадження результатів наукової розробки складала 1 шт., а прибуток, що його отримувало підприємство на одиницю продукції до впровадження результатів наукової розробки – 300 грн.

Потрібно спрогнозувати збільшення чистого прибутку підприємства від впровадження результатів наукової розробки у кожному році відносно базового.

Збільшення чистого прибутку підприємства $\Delta П_1$ протягом першого року складе:

$$\Delta П_1 = 300 \cdot 1 + (300 + 250) \cdot 550 = 302\,800 \text{ (грн.)}$$

Обчислимо збільшення чистого прибутку підприємства $\Delta П_2$ протягом другого року:

$$\Delta П_2 = 300 \cdot 1 + (300 + 250) \cdot (550 + 800) = 742\,800 \text{ (грн.)}$$

Збільшення чистого прибутку підприємства $\Delta П_3$ протягом третього року становитиме:

$$\Delta П_3 = 300 \cdot 1 + (300 + 250) \cdot (550 + 800 + 900) = 1\,237\,800 \text{ (грн.)}$$

Отже, розрахунки показують, що відповідно прогнозуванню комерційний ефект від впровадження розробки виражається у значному збільшенні чистого прибутку підприємства.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Основними показниками, які визначають доцільність фінансування наукової розробки певним інвестором, є абсолютна і відносна ефективність вкладених інвестицій та термін їх окупності.

Розрахунок ефективності вкладених інвестицій передбачає:

1-й крок. Розрахунок теперішньої вартості інвестицій PV, що вкладаються в наукову розробку.

Такою вартістю ми можемо вважати прогнозовану величину загальних витрат ЗВ на виконання та впровадження результатів НДДКР, тобто $ЗВ = PV = 276\,062{,}8 \text{ (грн.)}$

2-й крок. Розрахуємо очікуване збільшення прибутку $\Delta П_i$, що його отримає підприємство (організація) від впровадження результатів наукової розробки, для кожного із років, починаючи з першого року впровадження.

Таке збільшення прибутку також було розраховане нами раніше та становить:

$$\Delta П_1 = 302\,800 \text{ (грн)},$$
$$\Delta П_2 = 742\,800 \text{ (грн)},$$
$$\Delta П_3 = 1\,237\,800 \text{ (грн)}.$$

3-й крок. Будуємо вісь часу, на якій відображаємо всі платежі (інвестиції та прибутки), що мають місце під час виконання науково-дослідної роботи та впровадження її результатів.

Рисунок 4.1 характеризує рух платежів (інвестицій та додаткових прибутків).

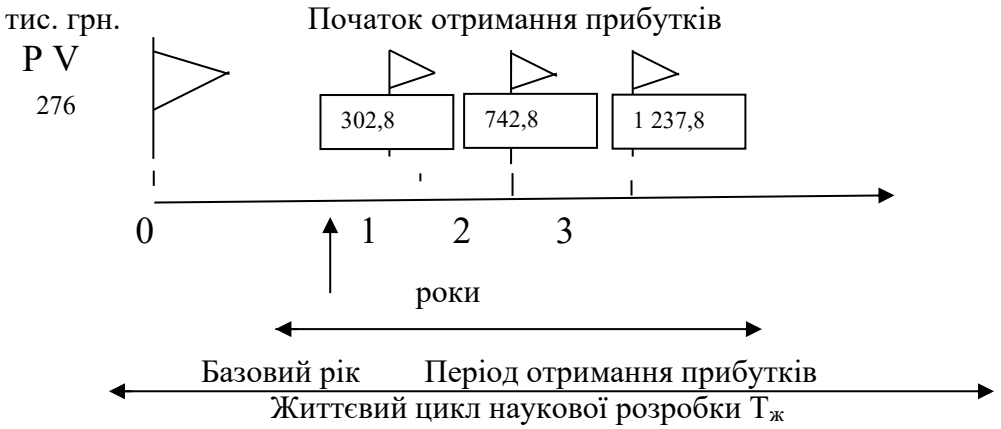


Рисунок 4.1 – Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДКР

4-й крок. Розрахуємо абсолютну ефективність вкладених інвестицій $Е_{абс}$ за формулою:

$$Е_{абс} = (ПП - PV), (грн.) \quad (4.8)$$

де ПП – приведена вартість всіх чистих прибутків, що їх отримає підприємство (організація) від реалізації результатів наукової розробки, грн.;

PV – теперішня вартість інвестицій $PV = ЗВ$, грн.

Приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, (грн) \quad (4.9)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн.;

Т – період часу, протягом якого виявляються результати впровадженої НДДКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні – 0,1;

t – період часу (в роках) від моменту отримання чистого прибутку до точки «0»;

$$ПП = \frac{302\,800}{(1+0{,}1)^1} + \frac{742\,800}{(1+0{,}1)^2} + \frac{1\,237\,800}{(1+0{,}1)^3} = 1\,819\,134\ (грн.)$$

$$Е_{абс} = 1\,819\,134 - 276\,062{,}8 = 1\,543\,071\ (грн.)$$

Оскільки $Е_{абс} > 0$, результат від проведення наукових досліджень щодо розробки програмного продукту та їх впровадження принесе прибуток, тобто є доцільним, проте це ще не свідчить про те, що інвестор буде зацікавлений у фінансуванні даної програми.

5-й крок. Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $Е_в$ за формулою:

$$Е_в = \sqrt[Т_ж]{1 + \frac{Е_{абс}}{PV} - 1} \quad (4.10)$$

де $Е_{абс}$ – абсолютна ефективність вкладених інвестицій, грн.;

PV – теперішня вартість інвестицій $PV = ЗВ, грн.$

$Т_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{1 + \frac{1\,543\,071}{276\,062{,}8}} - 1 = \sqrt[3]{6{,}59} - 1 = 0{,}82 \text{ або } 82\%$$

Порівняємо $E_в$ з мінімальною (бар'єрною) ставкою дисконтування τ_{min}, яка визначає ту мінімальну дохідність, нижче за яку інвестиції вкладатися не будуть.

Спрогнозуємо величину τ_{min}.

У загальному вигляді мінімальна (бар'єрна) ставка дисконтування

τ_{min}визначається за формулою:

$$\tau_{min} = d + f \quad (4.11)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; $d = 0{,}2$;

f – показник, що характеризує ризикованість вкладень;

величина $f = 0{,}5$.

$$\tau_{min} = 0{,}2 + 0{,}5 = 0{,}7$$

Оскільки $E_в = 82\% > \tau_{min} = 70\%$, то у інвестора є потенційна зацікавленість у фінансуванні даної наукової розробки.

6-й крок. Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій $Т_{ок}$ за формулою:

$$Т_{ок} = \frac{1}{Е_в}, \text{рік} \quad (4.12)$$

$$Т_{ок} = \frac{1}{0{,}82} = 1{,}2 \text{ (року)}$$

Оскільки термін окупності вкладених у реалізацію наукового проекту інвестицій менше трьох років ($Т_{ок} < 3$ років), то фінансування нової розробки є доцільним.

4.5 Висновки до розділу

В даному розділі було виконано оцінювання комерційного потенціалу розробки програмного засобу з використанням алгоритму для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

Проведено технологічний аудит з залученням трьох незалежних експертів. Визначено, що рівень комерційного потенціалу розробки вище середнього. Проведено порівняння з аналогами.

Згідно з проведеним оцінюванням нова розробка є якісною та конкурентоспроможною.

Рівень комерційного потенціалу розробки, становить 42 бали, що відповідає рівню «високий».

Згідно із розрахунками всіх статей витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи загальні витрати на розробку складають 276 062,8 (грн.). Розрахована абсолютна ефективність вкладених інвестицій в сумі 1 819 134 (грн.) свідчить про отримання прибутку інвестором від комерціалізації програмного продукту.

Щорічна ефективність вкладених в наукову розробку інвестицій складає 82%, що вище за мінімальну бар'єрну ставку дисконтування, яка складає 70%. Це означає потенційну зацікавленість інвесторів у фінансуванні розробки.

Термін окупності вкладених у реалізацію проекту інвестицій становить 1,2 (року), що також свідчить про доцільність фінансування нової розробки.

Отже, в результаті аналізу отриманих економічних показників, можна вважати, що запропонована розробка програмного засобу з використанням алгоритму для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

ВИСНОВОК

В даній роботі здійснювалась робота над підвищенням стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

Дана тема є на сьогодні актуальною, оскільки питання про визначення оригінальності документів, чи то фізичні документи (гроші, цінні та конфіденційні документи) або електронні документи (скановані копії, фотографії, електронний друкований текст) нині порушують дедалі частіше. Це викликано збільшенням обсягу документообігу між організаціями, а також розвитком технологій обміну документами. У зв'язку з цим з'являється безліч різних методів захисту документів від підробки.

Виходячи із поставленої мети та задач роботи, у першому розділі було здійснено аналіз галузі стеганографічної галузі та її методів з метою захисту даних, що містяться в електронному документообороті, досліджено застосування цифрового водяного знаку з метою захисту електронних документів від несанкціонованої модифікації, досліджено особливості стеганографічних систем, здійснено аналіз існуючих загроз для ЦВЗ та відповідно методів нанесення ЦВЗ з подальшим дослідженням їх переваг та недоліків.

В другому розділі роботи було описано запропоноване вдосконалення стеганографічного методу на основі алгоритму RDH, а саме його гістограмного типу оборотного зміщення. Оскільки, основна проблема даного типу полягає у значному погіршені якості стегоконтейнера, що призводить до зниження якості захисту (оскільки стають видимими вбудовані ЦВЗ), а також збільшенню візуальної помітності внесених змін, то відповідно, в якості удосконалення для коригування обраних пікселів гістограмного зміщення для розподілу вбудовуваних даних застосуємо метод дискретного вейвлет-перетворення із використанням модифікованих коефіцієнтів середньочастотної та

високочастотної областей. Щоб ускладнити візуальне сприйняття змін файлу-контейнера під час вбудовування ЦВЗ здійснюється додаткове закриття зображення адитивним шумом.

Виходячи із запропонованого удосконалення, в даному підрозділі була описана його математична модель, здійснена розробка алгоритму вбудовування цифрового водяного знаку у електронні документи формату jpeg та pdf, розробленого алгоритм роботи програмного додатку на основі вдосконаленого методу.

У третьому розділі на основі обраних засобів програмування таких як C#, Visual Studio 2022, Windows Forms та .NET Framework було здійснено програмну реалізацію додатку. В ході написання розділу було здійснено розробку користувацького інтерфейсу програмного додатку із врахуванням особливостей розробки; наведено основні фрагменти коду, що були написані для реалізації основного функціоналу розробки; описано інструкцію користувача для роботи з програмою. Отримані результати тестування свідчать про успішність вдосконаленого методу та доцільність його застосування на практиці. Вдосконалений метод на основі гістограмного типу має вищі якісні та кількісні показники порівняно з початковим методом, а стійкість алгоритму до впливів на стегоконтейнер підвищена орієнтовно на 7%. Тестування програмного додатку показало, що програма коректно працює на усіх версіях ОС Windows та може бути застосована на практиці в комерційних цілях.

В четвертому розділі роботи було виконано оцінювання комерційного потенціалу розробки програмного засобу , яке показало, що виконана робота має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

Аналізуючи отримані результати, можна вважати, що в ході виконання роботи досягнута її основна мета, а саме здійснено підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стеганографія. Навчальний посібник. веб-сайт. URL: http://tks.nau.edu.ua/wp-content/uploads/2016/05/Steganografiya.pdf (дата звернення: 02.05.2023).

2. Яремчук, Ю. Є., and В. В. Карпінець. "Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення." Інформаційні технології та компютерна інженерія.№ 1: 212-217. (2007).

3. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії : Навчальний посібник для студентів і аспірантів. – Вінниця:ВДТУ, 2003. – 143 с.

4. Основні механізми захисту електронних документів від фальсифікацій | Вісник Черкаського державного технологічного університету. Вісник Черкаського державного технологічного університету. URL: http://vtn.chdtu.edu.ua/article/view/82987 (дата звернення: 02.05.2023).

5. Методи і технології захисту інформації в системах електронного документообігу. ICI Journals Master List. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/635623.pdf (дата звернення: 02.05.2023).

6. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. – К.: НПУ імені М.П. Драгоманова, 2012. – 120 с.

7. W. Zeng, "Digital watermarking and data hiding: technologies and applications," in Proc. Int. Conf. Inf. Syst., Anal. Synth., vol. 3, 2018, pp. 223–229.

8. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Syst. J., vol. 35, no. 3–4, pp. 313–336, 2016.

9. J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in Proc. SPIE Security Watermarking Multimedia Contents, San Jose, CA, Jan. 2021, pp. 197–208.

10. Ingemar J.C., Joe K., and Thomson F.L. et al: ‘Secure spread spectrum watermarking for multimedia’, IEEE Trans. Image Process., 2017, 6, (12), pp. 1673–1687

11. Hao-Tian W., and Jiwu H.: ‘Reversible image watermarking on prediction errors by efficient histogram modification’, Signal Process., 2012, 92, (12), pp. 3000–3009

12. Su W., Wang X., and Li F. et al: ‘Reversible data hiding using the dynamic block-partition strategy and pixel-value-ordering’, Multimedia Tools Appl., 2019, 78, (7), pp. 7927– 7945

13. Лагун, А.В. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А.В. Лагун, І.А Лагун // Захист інформації і безпека інформаційних систем. – Львів, 2013. – С. 98 – 99.

14. Юдін, О.К., Захист інформації в мережах передачі даних : Підручник. / О.К. Юдін, Г.Ф. Конахович, О.Г.; під загальною редакцією Г.Ф. Корченко. –К. : ТОВ НВП «Інтерсервіс», 2009. –716 с.

15. Кінзерявий, О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень: дис. … канд. техн.. наук. Спеціальність 05.13.21 – Системи захисту інформації. Київ , 2015, 324 с.

16. Сучасні стеганографічні методи захисту інформації URL: https://www.researchgate.net/publication/311663916_sucasni_steganograficni_metodi_zahistu_informacii (дата звернення: 02.05.2023).

17. Стеганографічні методи захисту інформації – Wiki DonNTU. Wiki DonNTU. URL: https://wiki.donntu.edu.ua/view/Стеганографічні_методи_захисту_інформації (дата звернення: 02.05.2023).

18. Classifications steganography techniques. core – Aggregating the world’s open access research papers. URL: https://core.ac.uk/download/pdf/80501175.pdf (дата звернення: 02.05.2023).

19. Мельник С. Методи цифрової стеганографії: стан та напрями розвитку // С. Мельник, В. Кащук. // Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70;

20. Шелест М. Комп'ютерна стеганографія та її можливості // М. Шелест, В. Андрєєв. // Сучасна спеціальна техніка. – 2011. – №24. – С. 97–104.

21. Роль стеганографії у сучасному захисті інформації. LSULS Digital Repository: Home. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/7173/1/1.pdf (дата звернення: 02.05.2023).

22. Тарасов Д. О. Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д. О. Тарасов, А. С. Мельник, М. М. Голобородько // Інформаційні системи та мережі. Вісник НУ «Львівська політехніка». – 2010. – № 673. – С. 365–374.

23. Стасюк О. І. та ін. Сучасні стеганографічні методи захисту інформації / О. І. Стасюк та ін. // Захист інформації. – 2011. – Т. 13. – № 1 (50).

24. .Козіна М.О., Папковська О.Б., Логінова Н.І., Козін О.Б. Стеганоалгоритм, що використовує сингулярне розкладання матриці контейнера. Сучасний захист інформації. 2018. № 2. С.47-52.

25. Класифікація стеганографічних методів. Education and Science. URL: http://www.rusnauka.com/9_NND_2012/Informatica/4_105640.doc.htm (дата звернення: 02.05.2023).

26. Martin K. Що таке стеганографія та чим вона відрізняється від криптографії? 2023. instagalleryapp.com. URL: https://instagalleryapp.com/informacijna-bezpeka/shho-take-steganografija-ta-chim-vona/ (дата звернення: 02.05.2023).

27. Комп'ютерна стеганографія. StudFiles. URL: https://studfile.net/preview/9650047/page:7/ (дата звернення: 02.05.2023).

28. Chen LST, Lin SJ, Lin JC (2010) Reversible JPEG-based hiding method with high high hiding-ratio. Int J Pattern Recognit Artif Intell 24:433–456.

29. Celik MU, Sharma G, Tekalp AM, Saber E (2005) Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing 14:253–266.

30. M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, "Оборотне приховування даних", Proc. IEEE Image Process., vol. 2, pp. 157-160, 2002

31. J. Fridrich, M. Goljan and R. Du, "Invertible authentication", Proc. SPIE Security Watermarking Multimedia Contents, pp. 197-208

32. C. De Vleeschouwer, J. F. Delaigle and B. Macq, "Кругова інтерпретація гістограми для оборотного водяного знака", IEEE Int. Multimedia Signal Process. Семінар, с. 345-350

33. Кущ С. М. Виявлення прихованих повідомлень як складова комплексних систем захисту інформації / С. М. Кущ, В. М. Луценко, Д. О. Прогонов // Захист інформації. – 2012. № 3. – С. 65 – 71.

34. Що таке JPEG формат, його особливості. IT blog of the system administrator and programmer. URL: https://it-inzhener.com/uk/articles/detail/jpeg-format (дата звернення: 02.05.2023).

35. A. R. Calderbank, I. Daubechies, W. Sweldens and B. Yeo, "Wavelet transforms that map integers to integers", Appl. Comput., vol. 5, no. 3, pp. 332-369, 1998.

36. Що таке PDF-файл. Що таке PDF. Все про Android. URL: https://androidas.ru/what-is-a-pdf-document-what-is-pdf/ (дата звернення: 02.05.2023).

37. Вступ в C#. programm.top: веб-сайт. URL: https://programm.top/uk/c-sharp/tutorial/introduction/ (дата звернення: 24.10.2022).

38. Visual Studio: IDE and Code Editor for Software Developers and Teams. Visual Studio. URL: https://visualstudio.microsoft.com/en/ (дата звернення: 02.05.2023).

39. What is Windows Forms - Windows Forms .NET. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/dotnet/desktop/winforms/ (дата звернення: 02.05.2023).

40. NET Framework Microsoft. веб-сайт. URL: https://support.microsoft.com/microsoft-net-framework-9d23f658-3b97-68ab-d013-aa3c3e7495e0 (дата звернення: 24.10.2022).

41. Інформатика в прикладах - Основні компоненти програми для ОС з графічним інтерфейсом. Інформатика в прикладах - Головна. URL: http://nikolay.in.ua/distantsijne-navchannya/8-klas/840-osnovni-komponenti-programi-dlya-os-z-grafichnim-interfejsom (дата звернення: 02.05.2023).

42. Wikiwand - Графічний інтерфейс користувача. Wikiwand. URL: https://www.wikiwand.com/uk/Графічний_інтерфейс (дата звернення: 02.05.2023).

43. Графічний інтерфейс. Кафедра математичної фізики | Новини. URL: http://www.matfiz.univ.kiev.ua/userfiles/files/Pres20_cm.pdf (дата звернення: 02.05.2023).

44. Nayak MR, Tudu B, Basu A, Sarkar SK (2015) On the implementation of a secured digital watermarking frame work. Inf Secur J Glob Perspect 24(1):1– 9.

45. Gutierrez-Cardenas J.M. Steganography and data loss prevention: an overlooked risk? // International Journal of Security and Its Applications. 2017. V. 11. N 4. P. 71–84.

46. Miri A., Faez K. An image steganography method based on integer wavelet transform. Multimedia Tools and Applications. 2018. Vol. 77 (11). P 13133–13144.

47. Порівняння стійкості стеганографічних методів до різних типів спотворення програмними засобами | Системи обробки інформації. ХНУПС | Наукові видання. URL: https://journal-hnups.com.ua/index.php/soi/article/view/185 (дата звернення: 02.05.2023).

48. The System to Analyze of Stability of Robust Steganographic Algorithms. Neliti - Liberate Knowledge. URL: https://www.neliti.com/publications/305651/the-system-to-analyze-of-stability-of-algorithms (дата звернення: 02.05.2023).

49. Title. USENIX | The Advanced Computing Systems Association. URL: https://www.usenix.org/legacy/events/sec01/full_papers/provos/provos_html/ (дата звернення: 02.05.2023).

50. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ
Голова секції «Управління інформаційною
Безпекою» кафедри МБІС
д.т.н., професор
Юрій ЯРЕМЧУК
«25» березня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму

08-72.МКР.001.00.004.ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н., доцент Василь Карпінець

Вінниця – 2023 р.

1. Найменування та область застосування

Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ №68 від 20.03.2023р.

3. Мета та призначення розробки

3.1 Мета розробки: підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму.

3.2 Призначення: розроблений програмний засіб виконує захист лектронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму.

4. Джерела розробки

4.1. Стеганографія. Навчальний посібник. веб-сайт. URL: http://tks.nau.edu.ua/wp-content/uploads/2016/05/Steganografiya.pdf (дата звернення: 02.05.2023).

4.2. Яремчук, Ю. Є., and В. В. Карпінець. "Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення." ІТ та компютерна інженерія.№ 1: 212-217. (2007).

4.3. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп’ютерної стеганографії : Навчальний посібник для студентів і аспірантів. – Вінниця: ВДТУ, 2003. – 143 с.

4.4. Основні механізми захисту електронних документів від фальсифікацій | Вісник ЧДТУ. URL: http://vtn.chdtu.edu.ua/article/view/82987 (дата звернення: 02.05.2023).

4.5. Методи і технології захисту інформації в системах електронного документообігу. ICI Journals Master List. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/635623.pdf (дата звернення: 02.05.2023).

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів: процесор – Pentium 1500 МГц і подібні до них; оперативна пам’ять – не менше 512 Mb; середовище функціонування – операційна система сімейство Windows; вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов’язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.3.

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист відеофайлів від несанкціонованого копіювання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до онлайн-сервісу.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	25.03.2023	28.03.2023
2	Аналіз предметної області обраної теми	29.03.2023	10.04.2023
3	Апробація отриманих результатів	10.04.2023	15.04.2023
4	Розробка алгоритму роботи	16.04.2023	30.04.2023
5	Написання магістерської роботи на основі розробленої теми	01.05.2023	25.05.2023
6	Розробка економічної частини	26.05.2023	31.05.2023
7	Передзахист магістерської кваліфікаційної роботи	01.06.2023	10.06.2023
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	11.06.2023	19.06.2023
9	Захист магістерської кваліфікаційної роботи	20.06.2023	21.06.2023

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– програмний додаток;

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв Ю.П. Іщенко

Додаток Б. Лістинг файлу Steganography

```
using System;
using System.Drawing;
namespace Steganography
{
   class SteganographyHelper
   {
      enum State
      {
         hiding,
         filling_with_zeros
      };
      public static Bitmap embedText(string text, Bitmap bmp)
      {   State s = State.hiding;
         int charIndex = 0;
         int charValue = 0;
         long colorUnitIndex = 0;
         int zeros = 0;
         int R = 0, G = 0, B = 0;
         for (int i = 0; i < bmp.Height; i++)
         {          for (int j = 0; j < bmp.Width; j++)
            {
               Color pixel = bmp.GetPixel(j, i);
               pixel = Color.FromArgb(pixel.R - pixel.R % 2,
                  pixel.G - pixel.G % 2, pixel.B - pixel.B % 2);
               R = pixel.R; G = pixel.G; B = pixel.B;

               for (int n = 0; n < 3; n++)
               {
                  if (colorUnitIndex % 8 == 0)
                  {
                     if (zeros == 8)
                     {
                        if ((colorUnitIndex - 1) % 3 < 2)
                        {
                           bmp.SetPixel(j, i, Color.FromArgb(R, G, B));
                        }
                        return bmp;
                     }
                     if (charIndex >= text.Length)
                     {
                        s = State.filling_with_zeros;
                     }
                     else
                     {
                        charValue = text[charIndex++];
                     }
```

```
            }
            switch (colorUnitIndex % 3)
            {
               case 0:
                  {
                     if (s == State.hiding)
                     {
                        R += charValue % 2;

                        charValue /= 2;
                     }
                  }
                  break;
               case 1:
                  {
                     if (s == State.hiding)
                     {
                        G += charValue % 2;

                        charValue /= 2;
                     }
                  }
                  break;
               case 2:
                  {
                     if (s == State.hiding)
                     {
                        B += charValue % 2;

                        charValue /= 2;
                     }

                     bmp.SetPixel(j, i, Color.FromArgb(R, G, B));
                  }
                  break;
            }
            colorUnitIndex++;

            if (s == State.filling_with_zeros)
            {
               zeros++;
            }
         }
      }
   }
   return bmp;
}
public static string extractText(Bitmap bmp)
{
```

```
        int colorUnitIndex = 0;
        int charValue = 0;
        string extractedText = String.Empty;
        for (int i = 0; i < bmp.Height; i++)
        {
            for (int j = 0; j < bmp.Width; j++)
            {
                Color pixel = bmp.GetPixel(j, i);
                for (int n = 0; n < 3; n++)
                {
                    switch (colorUnitIndex % 3)
                    {
                        case 0:
                            {
                                charValue = charValue * 2 + pixel.R % 2;
                            }
                            break;
                        case 1:
                            {
                                charValue = charValue * 2 + pixel.G % 2;     }
                            break;
                        case 2:
                            {
                                charValue = charValue * 2 + pixel.B % 2;
                            }
                            break;          }
                    colorUnitIndex++;
                    if (colorUnitIndex % 8 == 0)
                    {   charValue = reverseBits(charValue);
                        if (charValue == 0)
                        {
                            return extractedText;
                        }
                        char c = (char)charValue;
                        extractedText += c.ToString();
                    }               }
            }         }
        return extractedText;
    }
    public static int reverseBits(int n)
    {
        int result = 0;
        for (int i = 0; i < 8; i++)
        {
            result = result * 2 + n % 2;
            n /= 2;         }
        return result;
    }
}}
```

Додаток В. Лістинг вдосконаленого алгоритму

```
using System;
using System.Collections;
using System.Drawing;
using System.Drawing.Imaging;
using System.Text;
using System.Windows.Forms;
namespace Steganography
{
   public partial class TextIntoImage : Form
   {
      public string key;

      public TextIntoImage()
      {
         InitializeComponent();
      }
      OpenFileDialog op = new OpenFileDialog();
      private void page_Closed(object sender, EventArgs e)
      {
         this.Hide();
         ImageHomePage sistema = new ImageHomePage();
         sistema.ShowDialog();
         this.Close();
      }
      private void textintoimage_Load(object sender, EventArgs e)
      {
      }
      private string myPath;
      private Guid myGuid;
      private FrameDimension myDimension;
      public ArrayList myImages = new ArrayList();
      private int myPageCount;
      private Bitmap myBMP;
      private void button1_Click(object sender, EventArgs e)
      {
         try
         {
            op.Filter = @"Image Files|*.png;";
            op.ShowDialog();
            if (string.IsNullOrEmpty(op.FileName))
               return;
            pictureBox1.Image = Image.FromFile(op.FileName);
            pictureBox1.SizeMode = PictureBoxSizeMode.StretchImage;
            Bitmap kk = new Bitmap(pictureBox1.Image, new Size(pictureBox1.Width,
pictureBox1.Height));
```

```
            Graphics g = Graphics.FromImage(kk);
            int iii = kk.Height / 8;
            int jjj = kk.Width / 8;
            pictureBox1.Image = kk;
            pictureBox1.SizeMode = PictureBoxSizeMode.StretchImage;
          }
          catch
          {
          }
        }
        private void button2_Click_1(object sender, EventArgs e)
        {
          Bitmap bmp = (Bitmap)pictureBox1.Image;
          byte[] bytes = Encoding.Default.GetBytes(textBox1.Text);
         var myString = Encoding.UTF8.GetString(bytes);
            string text = $"{key}:value{myString}";
          bmp = SteganographyHelper.embedText(text, bmp);
          try
          {
            SaveFileDialog sv = new SaveFileDialog();
            sv.Filter = @"Image Files|*.png;";
            sv.FileName = "result.png";
            sv.ShowDialog();
            if (!string.IsNullOrEmpty(sv.FileName))
            {
              bmp.Save(sv.FileName, System.Drawing.Imaging.ImageFormat.Png);
            }
          }
          catch (Exception ex)
          {
            MessageBox.Show(ex.ToString());
          }
          leastsignificantbit ls = new leastsignificantbit();
          ls.pic = pictureBox1;
          ls.Show();

        }
      }
    }


using System;
using System.Drawing;
using System.Windows.Forms;
namespace Steganography
{
  public partial class TextFromImage : Form
  {
    OpenFileDialog op = new OpenFileDialog();
```

```
        public TextFromImage()
        {
            InitializeComponent();
        }
        public string Key;
        private void page_Closed(object sender, EventArgs e)
        {
            this.Hide();
            ImageHomePage sistema = new ImageHomePage();
            sistema.ShowDialog();
            this.Close();
        }
        private void button1_Click_1(object sender, EventArgs e)
        {           try
            {
                op.ShowDialog();
                op.Filter = @"Image Files|*.png;";
                pictureBox1.Image = Image.FromFile(op.FileName);
                pictureBox1.SizeMode = PictureBoxSizeMode.StretchImage;
                textBox1.Text = "";
            }
            catch
            {
            }       }
        private void button2_Click_1(object sender, EventArgs e)
        {
            Bitmap bmp = (Bitmap)pictureBox1.Image;
            string extractedText = SteganographyHelper.extractText(bmp);
         var s = extractedText.Split(':');
            if (string.IsNullOrEmpty(s[0]) || s.Length<=1 || !s[1].StartsWith("value"))
            {
                MessageBox.Show(@"Ключова фраза не розпізнана. Файл зазнав
модифікації.");
                return;           }
            if (s.Length < 2 || s[0] != Key)
            {
                MessageBox.Show(@"Невірний ключ");
                return;           }
          var val = s[1].Replace("value", "");
            textBox1.Text = val;        }
        private void textBox1_TextChanged(object sender, EventArgs e)
        {       }
        private void pictureBox1_Click(object sender, EventArgs e)
        {
        }
        private void TextFromImage_Load(object sender, EventArgs e)
        {
        }    }
    }
```

Додаток Г. Інтерфейс програмного додатку

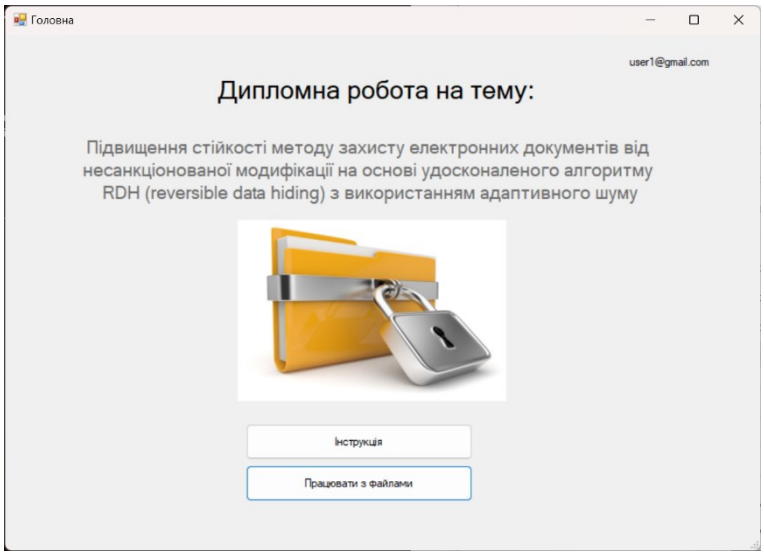


Рисунок 1 – Вигляд головного вікна додатку авторизованого користувача

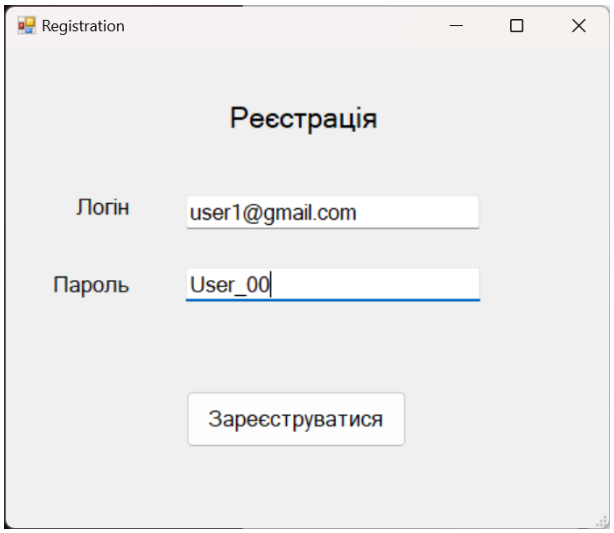


Рисунок 2 – Вигляд вікна реєстрації користувача

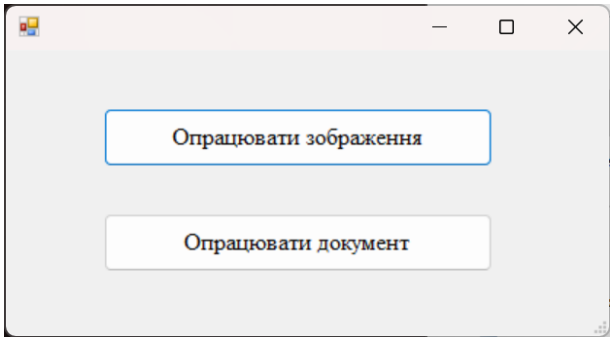


Рисунок 3 – Вигляд вікна для вибору формату файлу для подальшої роботи

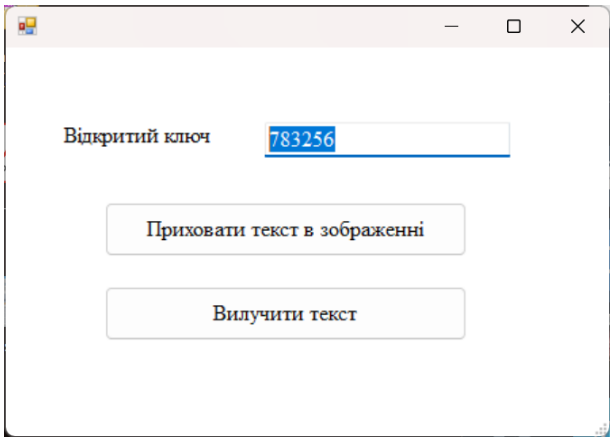


Рисунок 4 – Вигляд вікна для вибору відповідної функції

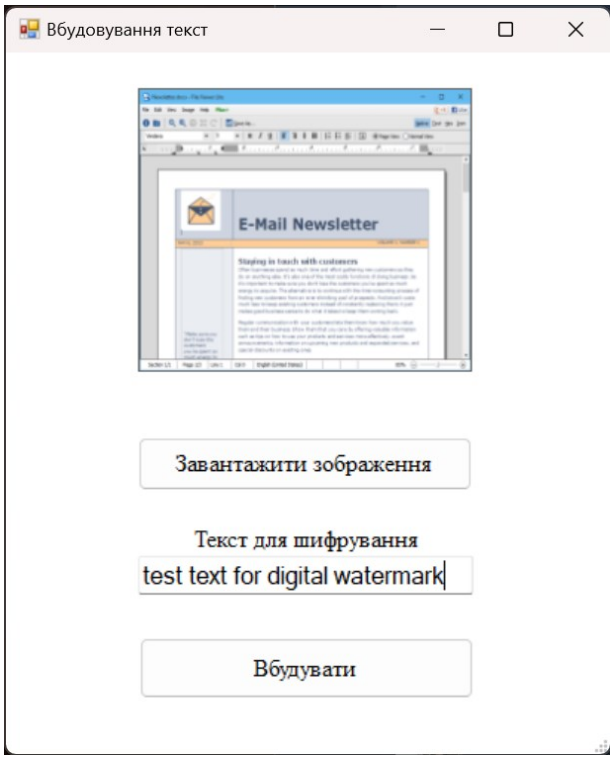


Рисунок 5 – Вигляд вікна для опрацювання файлу

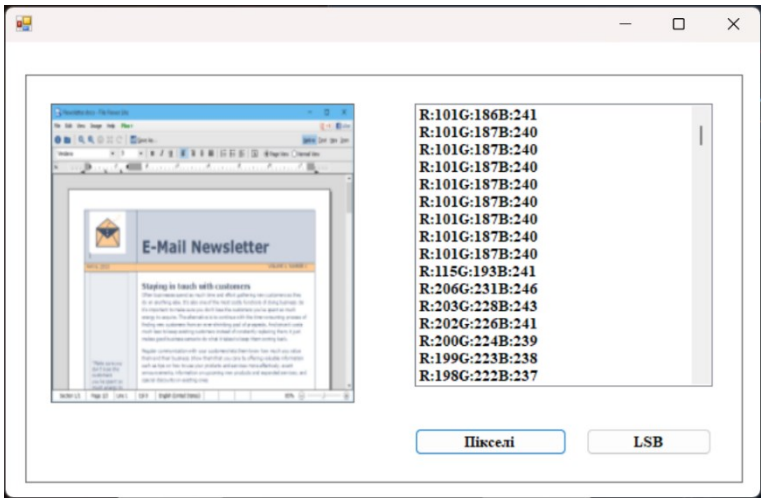


Рисунок 6 – Вигляд вікна із відображенням внесених змін за вдосконаленим алгоритмом

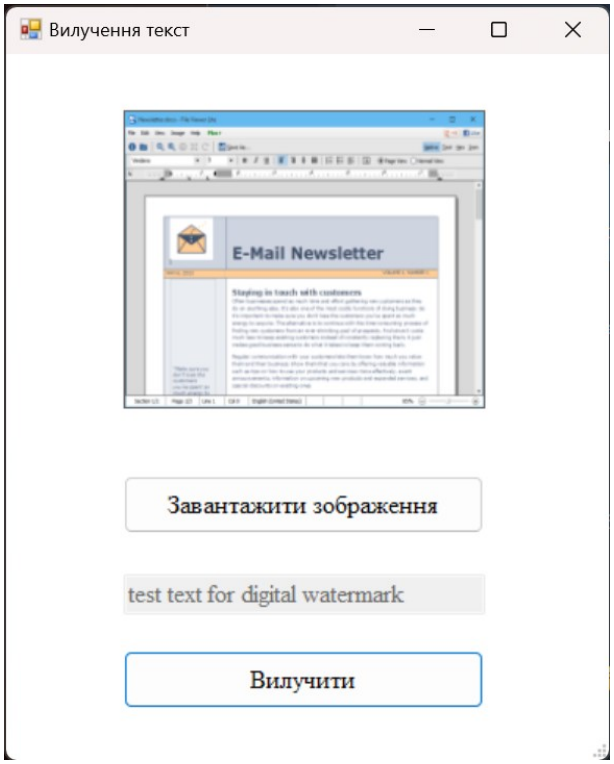


Рисунок 7 – Вигляд вікна для вилучення даних із зображення

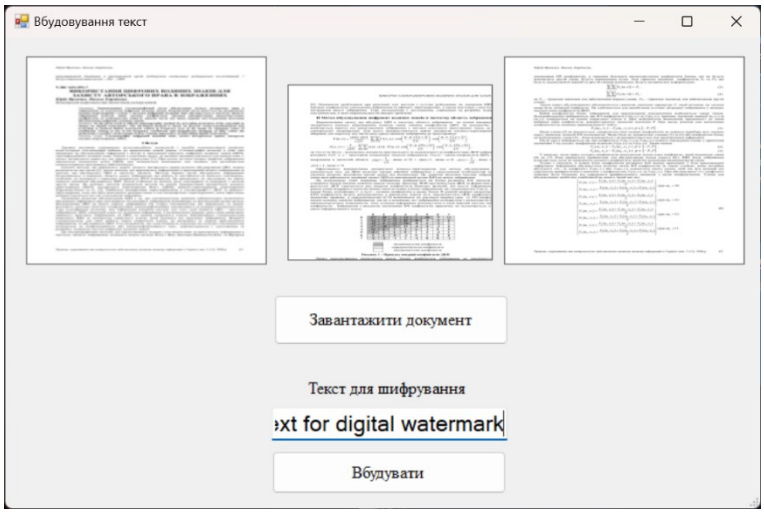


Рисунок 8 – Вигляд вікна із завантаженим файлом для опрацювання

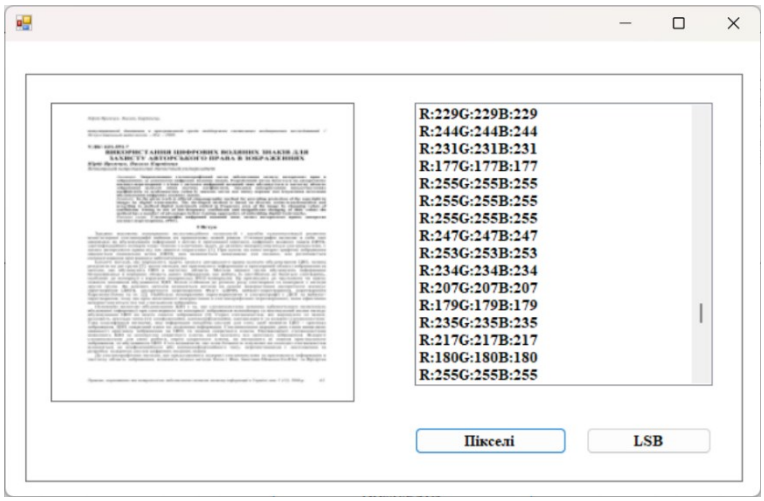


Рисунок 9 – Вигляд вікна із відображенням внесених змін за вдосконаленим алгоритмом

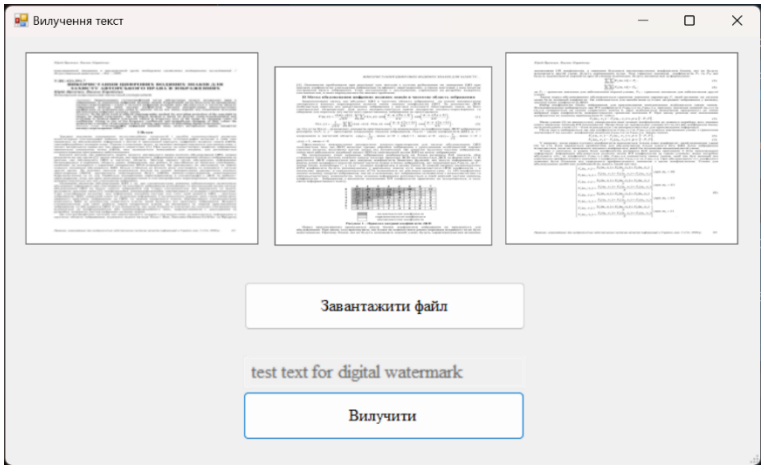


Рисунок 10 – Вигляд вікна для вилучення даних із зображення

Додаток Д. Ілюстративний матеріал

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему:

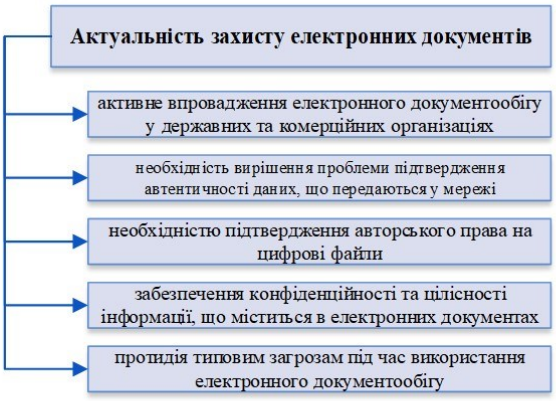
Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму

ВИКОНАВ: СТ. 2-ГО КУРСУ, ГРУПИ УБ-21МЗ
ІЩЕНКО ЮРІЙ ПЕТРОВИЧ
КЕРІВНИК: К.Т.Н., ДОЦ., ДОЦЕНТ КАФ. МБІС
КАРПІНЕЦЬ ВАСИЛЬ ВАСИЛЬОВИЧ

Актуальність та новизна роботи

Метою роботи є підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH з використанням адаптивного шуму.

Наукова новизна: вдосконалення алгоритму RDH з використанням адаптивного шуму з метою підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації.



Аналіз застосування цифрової стеганографії

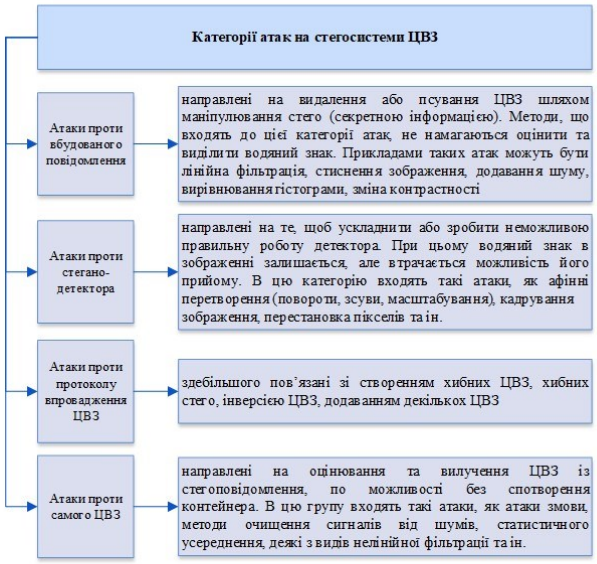
Цифрова стеганографія – це розділ стеганографії, що вивчає надійне приховування певних бітових послідовностей в стеганоконтейнерах (фото, документи, аудіо-файли).

Мета захисту	Галузь застосування
Захист від копіювання	Електронна комерція, контроль за копіюванням DVD, розповсюдження мультимедійної інформації
Прихована анотація документів	Медичні знімки, картографія, мультимедійні база даних
Аутентифікація	Системи відеоспостереження, електронні комерції, голосова пошта, електронне конфіденційне діловодство
Прихований зв'язок	Воєнні та розвідувальні додатки, а також застосування у випадках, коли неможливе застосування криптографічних методів

Аналіз застосування ЦВЗ для захисту електронних документів

Цифровий водяний знак (ЦВЗ) являє собою дані, що впроваджуються в інформаційний об'єкт з метою контролю його використання.

Технологія ЦВЗ заснована на застосуванні стеганографічних прийомів, у рамках яких приховується факт наявності ЦВЗ в інформаційному об'єкті (контейнері).



Аналіз існуючих методів захисту електронних документів

Узагальнений алгоритм вбудовування цифрових водяних знаків може бути представлений у вигляді математичної моделі побудови алгоритмів, стійких до цифро-аналогових перетворень завдяки врахуванню параметрів друкарського і скануючого пристрою (роздільна здатність).

Вдосконалення методу захисту електронних документів

Одним із найперспективніших методів, що вбудовує ЦВЗ в електронні документи різних форматів, є ***метод оборотного приховування даних (RDH, reversible data hiding).***

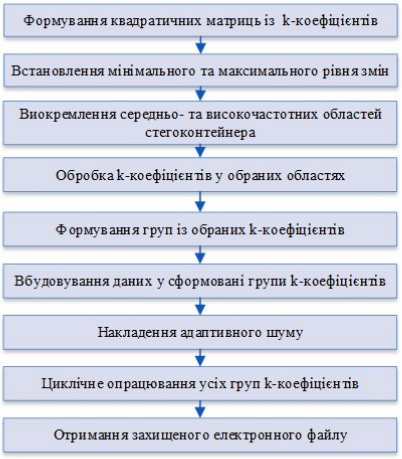
Даний метод використовується для забезпечення цілісності цифрового водяного знаку і контейнера.

Основна проблема даного типу полягає у значному погіршені якості стегоконтейнера, що призводить до зниження якості захисту (оскільки стають видимими вбудовані ЦВЗ), а також збільшенню візуальної помітності внесених змін.

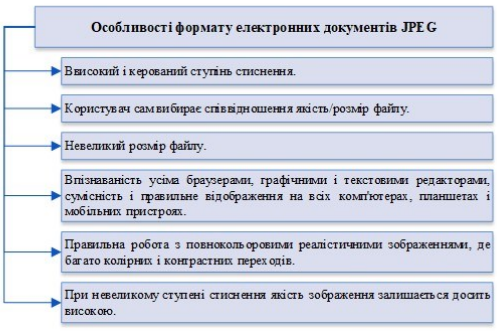
Алгоритм вбудовування ЦВЗ за вдосконаленим методом

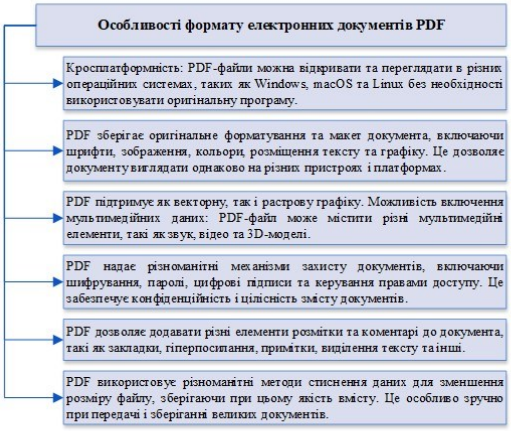
Для коригування обраних пікселів гістограмного зміщення для розподілу вбудовуваних даних ***застосуємо метод дискретного-вейвлет перетворення із використанням модифікованих коефіцієнтів середньочастотної та високочастотної областей.***

Щоб ускладнити візуальне сприйняття змін файлу-контейнера під час вбудовування ЦВЗ здійснюється ***додаткове закриття зображення адаптивним шумом.***



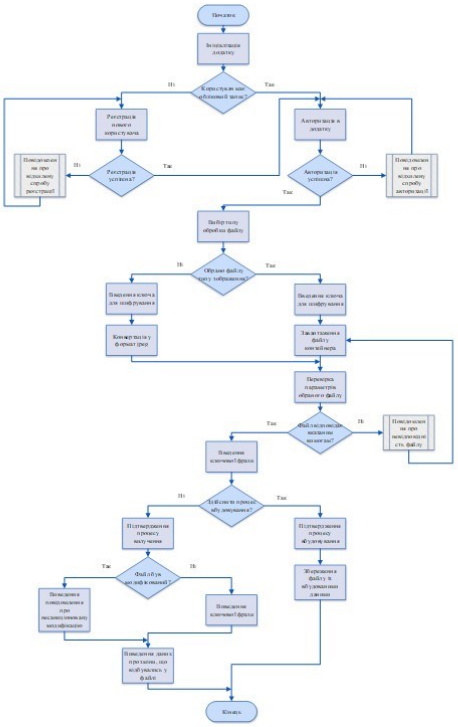
Вибір формату електронних документів для роботи





Розробка алгоритму роботи програмного додатку

На основі вдосконаленого методу захисту електронних документів від несанкціонованої модифікації ***розроблено програмний додаток,*** функціоналом якого передбачена можливість вбудовування та вилучення цифрового водяного знаку із використанням ключової зашифрованої фрази та можливістю перегляду внесених змін у файл у випадку його модифікації.

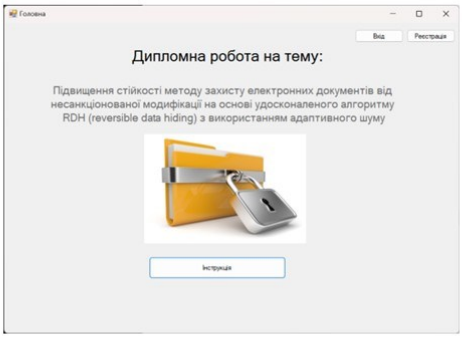


Вибір засобів програмування

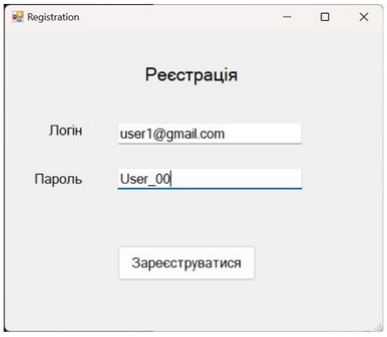
Виходячи із поставлених завдань роботи, для реалізації програмного додатку обрано наступні ***програмні засоби:***

- мова об'єктно-орієнтованого програмування ***C#;***
- середовище програмування ***Visual Studio 2022;***
- інтерфейс програмування додатків **Windows Forms;**
- програмна технологія для створення додатків ***.NET Framework.***

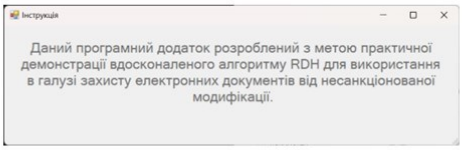
Інтерфейс програмного додатку



Вигляд головного вікна додатку

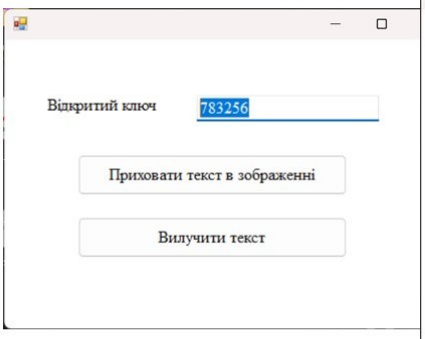


Вигляд вікна реєстрації користувача

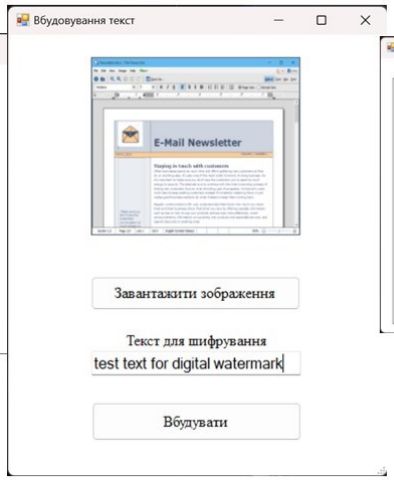


Вигляд вікна з додатковою інформацією

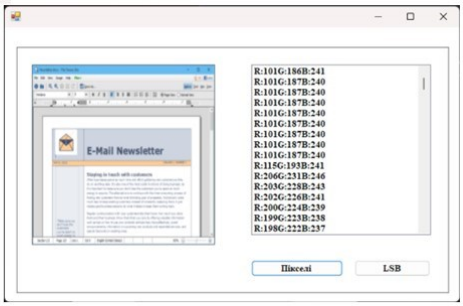
Інтерфейс програмного додатку



Вигляд вікна для вибору відповідної функції

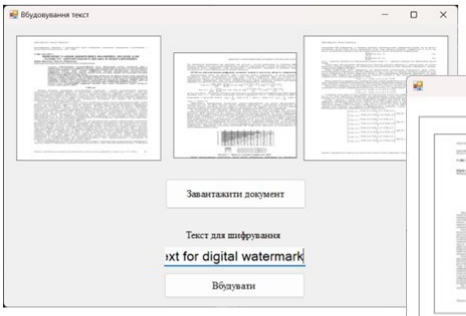


Вигляд вікна для опрацювання файлу

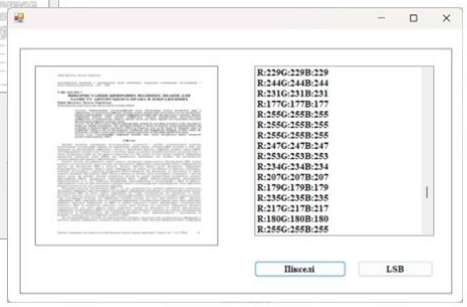


Вигляд вікна із відображенням внесених змін за вдосконаленим алгоритмом

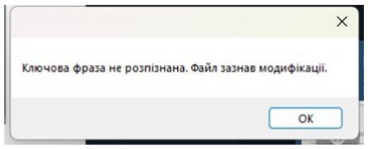
Інтерфейс програмного додатку



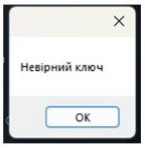
Вигляд вікна із завантаженим файлом для опрацювання



Вигляд вікна із відображенням внесених змін за вдосконаленим алгоритмом



Сповіщення про спробу модифікації файлу



Сповіщення про некоректний ключ для опрацювання файлу

Тестування. Стійкість методів до спотворення рівномірним шумом

Метод	Рівень рівномірного шуму								
	10	20	30	40	50	65	75	85	100
Вдосконалений метод	0	0	0	0	0	0	0,01	0,1	0,16
Гістограмний метод	0	0	0	0	0,01	0,12	0,13	0,19	0,22
Метод випадкових інтервалів	0	0	0	0	0	0,06	0,1	0,23	0,33
Метод блокового приховування	0	0	0	0,05	0,1	0,15	0,18	0,2	0,23

Тестування. Стійкість методів до jpeg-стиснення

Метод	Коефіцієнт якості jpeg-стиснення								
	100	85	75	60	50	40	30	20	10
Вдосконалений метод	0	0	0	0	0,03	0,1	0,25	0,37	0,42
Гістограмний метод	0	0	0	0,05	0,11	0,21	0,28	0,43	0,51
Метод випадкових інтервалів	0	0	0	0,06	0,14	0,19	0,26	0,37	0,45
Метод блокового приховування	0	0,01	0,06	0,1	0,13	0,2	0,32	0,41	0,53

Тестування. Дослідження показників PSNR, AD, SSIM

Тестування. Робастність ЦВЗ

Метод	Обрізання файлу	Повороти / віддзеркалення	Зміна яскравості	Надання чорно-білого відтінку	Згладжу-вання медіаним фільтром
Вдосконалений метод	92%	95%	97%	96%	93%
Гістограмний метод	85%	88%	91%	90%	83%
Метод випадкових інтервалів	84%	85%	93%	87%	82%
Метод блокового приховування	82%	81%	89%	85%	82%

Тестування. Візуальні зміни


Зображення без вбудованого ЦВЗ (оригінал) (зверху)


Зображення із вбудованим ЦВЗ (контейнер) (знизу)

Економічна доцільність розробки

Проведено дослідження економічного потенціалу розробки, зокрема, оцінювання комерційного потенціалу; прогнозування витрат на виконання наукової роботи та впровадження її результатів; прогнозування комерційних ефектів від реалізації результатів розробки та розрахунок ефективності вкладених інвестицій та періоду їх окупності.

В результаті аналізу отриманих економічних показників, можна вважати, що запропонована розробка програмного засобу з використанням алгоритму для підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

Висновки

Враховуючи актуальність обраної теми, в роботі було ***здійснено підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації.***

Запропоноване вдосконалення стеганографічного методу на основі алгоритму RDH, а саме його гістограмного типу оборотного зміщення. Оскільки, основна проблема даного типу полягає у значному погіршені якості стегоконтейнера, що призводить до зниження якості захисту, то в якості удосконалення для коригування обраних пікселів гістограмного зміщення для розподілу вбудовуваних даних ***застосовано метод дискретного-вейвлет перетворення із використанням модифікованих коефіцієнтів середньочастотної та високочастотної областей.*** Щоб ускладнити візуальне сприйняття змін файлу-контейнера під час вбудовування ЦВЗ ***здійснюється додаткове закриття зображення адитивним шумом.***

Розроблено програмний додаток на основі вдосконаленого методу. Отримані результати тестування свідчать про успішність вдосконаленого методу та доцільність його застосування на практиці. Вдосконалений ***метод має вищі якісні та кількісні показники порівняно з початковим методом,*** а стійкість алгоритму до впливів на стегоконтейнер ***підвищена орієнтовно на 7%.***

Дякую за увагу!

Додаток Е. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ
ЗАПОЗИЧЕНЬ

Назва роботи:
Підвищення стійкості методу захисту електронних документів від несанкціонованої модифікації на основі удосконаленого алгоритму RDH (reversible data hiding) з використанням адаптивного шуму
Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 92% Схожість 8%

Аналіз звіту подібності (відмітити потрібне):
1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Коваль Н.П.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Іщенко Ю.П.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Карпінець В.В.
(підпис) (прізвище, ініціали)