Міністерство освіти і науки України
Одеський національний політехнічний університет
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки і програмного забезпечення

Варда Тамара Володимирівна,
студентка групи РЗ-151

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

Розробка стеганографічного методу, стійкого до атак проти вбудованого повідомлення

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Кобозєва Алла Анатоліївна,
д.т.н., професор

Одеса – 2020

Міністерство освіти і науки України
Одеський національний політехнічний університет
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра інформатики та управління захистом інформаційних систем
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІУЗІС

_____
д.т.н.,проф. А.А.Кобозєва
____ _____202_р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Варді Тамарі Володимирівні

1.Тема роботи: *Розробка стеганографічного методу, стійкого до атак проти вбудованого повідомлення*,

керівник роботи *Кобозєва Алла Анатоліївна, д.т.н., проф,*

затверджені наказом ректора ОНПУ від „____”_____ 20___ р. №_____ .

2.Зміст роботи*: аналіз проблемної області, визначення формальних параметрів для розробки стеганографічного алгоритму, розробка стеганоалгоритму стійкого до атак проти вбудованого повідомлення, обчислювальний експеримент в умовах атаки стиском та накладання шумів, охорона праці.*

3. Перелік ілюстративного матеріалу: *Основні елементи стеганосистеми, ілюстрації роботи програмного інтерфесу: головне вікно, завантаження зображення, переведення секретного повідомлення у ДІ, результат стеганоперетворення, результат декодування ДІ та ілюстрації використання програмного забезпечення.*

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці	Ярова І.А., к.т.н., доцент	Завдання видав	Завдання прийняв

6. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*1.09-15.09.2020*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*15.09-1.10.2020*	*виконано*
3	*Визначення формальних параметрів ЦЗ*	*1.10-20.10.2020*	*виконано*
4	*Розробка стенографічного алгоритму*	*20.10-10.11.2020*	*виконано*
5	*Оцінка ефективності розробленого алгоритму*	*10.11-25.11.2020*	*виконано*
6	*Підготовка тексту роботи*	*25.11-15.11.2020*	*виконано*
7	*Підготовка презентації та доповіді*	*15.11-20.112020*	*виконано*
8	*Попередній захист*	*1.12.2020*	*виконано*
9	*Нормоконтроль, рецензування*	*15.12.2020*	*виконано*
10	*Занесення роботи в електронний архів*	*20.12.2020*	*виконано*
11	*Допуск до захисту у завідувача кафедри*	*20.12.2020*	*виконано*

Здобувач вищої освіти _____ *Варда Т.В.*

Керівник роботи _____ *Кобозєва А.А.*

ЗАВДАННЯ

на розробку розділу “Охорона праці та безпека в надзвичайних ситуаціях”

Варді Тамарі Володимирівні, група РЗ-151

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки і програмного забезпечення

Тема роботи: *Розробка стеганографічного методу, стійкого до атак проти вбудованого повідомлення*

Зміст розділу:

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

Керівник роботи	Консультант з охорони праці та БНС
_____	_____
(прізвище та ініціали)	(прізвище та ініціали)
_____	_____
(підпис)	(підпис)
«____» _____ 2020 р.	«____» _____ 2020 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему “Розробка стеганографічного методу, стійкого до атак проти вбудованого повідомлення” на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 – Кібербезпека, освітня програма: «Кібербезпека», містить 12 рисунків, 5 таблиць, 1 додаток, 47 літературних джерел за переліком посилань. Робота виконана на 58 сторінках загального тексту і 50 сторінках основного тексту.

Метою роботи є підвищення ефективності прихованого каналу зв’язку шляхом розробки нового стеганографічного методу, стійкого до атак проти вбудованого повідомлення.

В роботі проведено аналіз предметної області, обрані параметри для стеганоперетворення, стійкого до атаки проти вбудованого повідомлення, наведені результати обчислювального експерименту та порівняння ефективності розробленого алгоритму з сучасними аналогами.

У результаті виконання кваліфікаційної роботи на основі властивостей сингулярних чисел блоків матриці контейнера розроблено стеганографічний метод, який в якості контейнера використовує цифрове зображення, стійкий до атаки проти вбудованого повідомлення, та його алгоритмічна реалізація, ефективність якої в умовах стиску стеганоповідомлення з втратами для деяких параметрів стиску перевищує найкращі аналоги, що дозволило підвищити ефективність прихованого каналу зв’язку.

Результати даної роботи можуть бути використані для організації стійкого прихованого каналу зв’язку в умовах можливих атак проти вбудованого повідомлення.

СТЕГАНОГРАФІЧНИЙ МЕТОД, СТІЙКІСТЬ ДО АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ, АТАКА СТИСКОМ, АТАКА НАКЛАДАННЯМ ШУМУ, СИНГУЛЯРНІ ЧИСЛА.

ANOTATION

Qualification work on "Development of steganographic method, resistant to attacks against embedded message" for the second (Master's) level of higher education in the specialty 125 - Cybersecurity, educational program "Cybersecurity", contains 12 figures, 5 tables, 1 appendix, 47 literature sources on the list of references. The work is realized on 58 pages of the general text and 50 pages of the main text.

The aim of the work is to improve the efficiency of covert communication channel by developing a new steganographic method resistant to attacks against embedded message.

In the work an analysis of the subject area, the selected parameters for the steganographic transformation, resistant to attack against embedded messages are the results of the computational experiment and comparison of the effectiveness of the developed algorithm with modern counterparts.

As a result of qualification work on the basis of properties of singular numbers of blocks of the container matrix has developed steganographic method, which uses a digital image as a container, resistant to attack against embedded messages and its algorithmic implementation, whose efficiency in terms of lossy compression steganopovideniya for some compression parameters exceeds the best analogues, thus improving the efficiency of the covert communication channel.

The results of this work can be used to organize a stable covert communication channel under conditions of possible attacks against the embedded message.

STEGANOGRAPHIC METHOD, STABILITY TO INTEGRATED MESSAGE ATTACS, COMPRESSION ATTACS, NOISE ATTACK, SINGULAR NUMBERS.

ЗМІСТ

ВСТУП

Інформація один з найцінніших людський ресурсів, отримати доступ до якого з появою глобальної мережі Інтернет стало значно простіше та швидше. Разом з цим зросла загроза несанкціонованого доступу до конфіденційної інформації, порушення авторських прав та інтелектуальної власності. Рішення цих проблем сьогодні головним чином лягає на криптографію та стеганографію.

Криптографія захищає інформацію, шифруючи її, тим самим роблячи незрозумілою при виявленні. На відміну від першої, стеганографія приховує сам факт існування секретного повідомлення. Це реалізується шляхом занурення додаткової інформації у об’єкти, що не привертають ніякої додаткової уваги, які потім пересилаються по каналам загального користування чи зберігаються в такому виді. Але питання захисту інформації на сьогоднішній день вимагає комплексного підходу та сумісного використання методів криптографії та стеганографії.

Розвиток інформаційних технологій, що вже увійшли у всі сфери життя людини, вплинув і на обсяг цифрової інформації, що стрімко збільшився за останнє десятиліття. Сьогодні цифрова інформація займає дуже велику роль у житті сучасної людини. Починаючи з електронних книг, музики, фільмів, закінчуючи фотографіями та відео, які можна вже зробити будь-де і будь-коли. Все ці мультимедійні дані займають значний обсяг пам’яті на пристроях та у хмарних сховищах. Для вирішення цієї проблеми були створені формати зберігання даних з втратами, які дозволяють скоротити об’єм інформації, що зберігається, майже не втрачаючи якість. Зменшення розміру файлів відбувається за рахунок видалення певних елементів, що залишаються непомітні оку людини, але для стеганографії це має негативні наслідки, адже можуть бути видалені елементи, у які була занурена секретна інформація. Тому для сучасних стеганографічних алгоритмів, окрім існуючих вимог, таких як прийнятна пропускна спроможність прихованого каналу зв’язку та надійність сприйняття стеганоповідомлення, висувається ще одна важлива вимога – стійкість до атак

проти вбудованого повідомлення, зокрема, до атаки стиском, яка є найбільш розповсюдженою. Саме це стало поштовхом для активного розвитку стеганографічних алгоритмів, стійких до атак проти вбудованого повідомлення.

Метою роботи є підвищення ефективності прихованого каналу зв'язку шляхом розробки нового стеганографічного методу, стійкого до атак проти вбудованого повідомлення.

Задачі, які необхідно вирішити для досягнення мети:

1. Обґрунтувати вибір формальних параметрів цифрового зображення, які задіюються при вбудові та аналізуються при декодуванні додаткової інформації, та їх кількісні характеристики;
2. Розробити стеганографічний метод та його алгоритмічну реалізацію;
3. Обґрунтувати стійкість до атак проти вбудованого повідомлення запропонованого стеганоперетворення;
4. Провести аналіз ефективності розробленого стеганографічного алгоритму, в тому числі порівняльний з сучасними аналогами.

Об'єктом досліджень є процес організації прихованого (стеганографічного) каналу зв'язку.

Предмет досліджень є стеганографічні методи, стійкі до атак проти вбудованого повідомлення.

Методи дослідження: теорія збурень, матричний аналіз, методи цифрової обробки зображення.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Основні поняття стеганографії. Вимоги до стеганосистем

Питання захисту інформації від несанкціонованого доступу встало ще в давні часи, а з появою та бурхливим розвитком інформаційних технологій воно стає все більш актуальним [1-3].

У стародавні часи для передачі секретної інформації робили татуювання на голові рабів, яких перед тим голили, далі чекали поки волосся відросте та відправляли їх у дорогу. Також у Давній Греції використовували дощечки для передачі таємних послань, які покривались воском та відправлялись. Або ж використовували симпатичні, так звані невидимі, чорнила, які при безпосередньому запису невидимі, але виявлялися лише за певних умов, таких як нагрів, вплив хімічних речовин, освітленні тощо [4].

Далі з розвитком людства та нових технологій стеганографія відкривала нові напрямки, тому сьогодні на ряду з класичною стеганографією існують комп’ютерна та цифрова стеганографія [5].

Під класичною розуміють ту, де для передачі інформації використовували технічні засоби захисту інформації [6].

Комп’ютерна стеганографія використовує спеціальні властивості форматів [7]. Цифрова стеганографія заснована на надмірності мультимедійних даних, що мають аналогову природу, такі як аудіофайли, зображення та відеопослідовності [8, 9]. Найбільш розповсюдженим об’єктом для вбудовування інформації є зображення, яке і буде досліджуватися у роботі.

Цифрова стеганографія – це наука про непомітне і надійне приховування одних бітових послідовностей в інших, що мають аналогову природу [10].

Цифрова стеганографія включає в себе наступні напрямки [10]:

- вбудовування інформації з метою її прихованої передачі;
- вбудовування цифрових водяних знаків (ЦВЗ) (watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting);
- вбудовування заголовків (captioning).

У зв'язку з активним розвитком інформаційних технологій досить гостро постало питання захисту від порушень авторських прав та інтелектуальної власності. Одним з найбільш ефективних способів захисту цифрової інформації є вбудова невидимих міток – ЦВЗ, що містять деякий автентичний код, наприклад інформацію про власника, та при аналізі спеціальним декодером одержуються рішення про їх справжність. Даний напрям знайшов широке застосування для захисту цифрових об'єктів від копіювання та несанкціонованого використання [10].

Вбудова в цифрові об’єкти ідентифікаційних номерів досить схожа з технологією ЦВЗ, основною відмінною рисою є унікальність кожного окремого вбудованого номеру. Так при порушенні прав, виробник точно може визначити яка з копій була незаконно скопійована і / або поширена [10].

Вбудовування заголовків здебільшого використовується в медицині, наприклад, для підпису цифрових медичних знімків чи нанесення легенд на карту пацієнта. Метою цієї технологіє є зберігання всієї різнорідної інформації в єдине ціле.

У 1996 році на науковій конференції Information Hiding: First Information Workshop [11], було винесено пропозицію про використання єдиної термінології і обговорені основні терміни.

Стеганографічна система або стеганосистема - це сукупність засобів і методів, які використовуються з метою формування прихованого (непомітного) каналу передачі інформації. [11,12].

На сьогодні стеганосистеми активно застосовуються для розв’язання таких ключових завдань [1-4]:

- захист конфіденційної інформації від несанкціонованого доступу;
- захист авторського права на інтелектуальну власність;
- захист комерційної, банківська, службової та державної таємниці.

Для того, щоб стегосистеми була надійною, необхідно виконання при її проектуванні ряду вимог [13,10]:

– Безпека системи повинна повністю визначатися секретністю ключа. Знання порушником факту наявності повідомлення в будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.

– Заповнений контейнер повинен бути візуально не відрізняється від незаповненого.

– Стегосистеми ЦВЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, його що не містить. У деяких додатках таке виявлення може призвести до серйозних наслідків. Наприклад, помилкове виявлення ЦВЗ на DVD-диску може викликати відмову від його відтворення плеєром.

– Повинна забезпечуватися необхідна пропускна здатність.

– Стегосистеми повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стегокодер і простий стегодекодер.

Основні елементи, що входять у стеганосистему зображені на рисунку 1.1 [10].

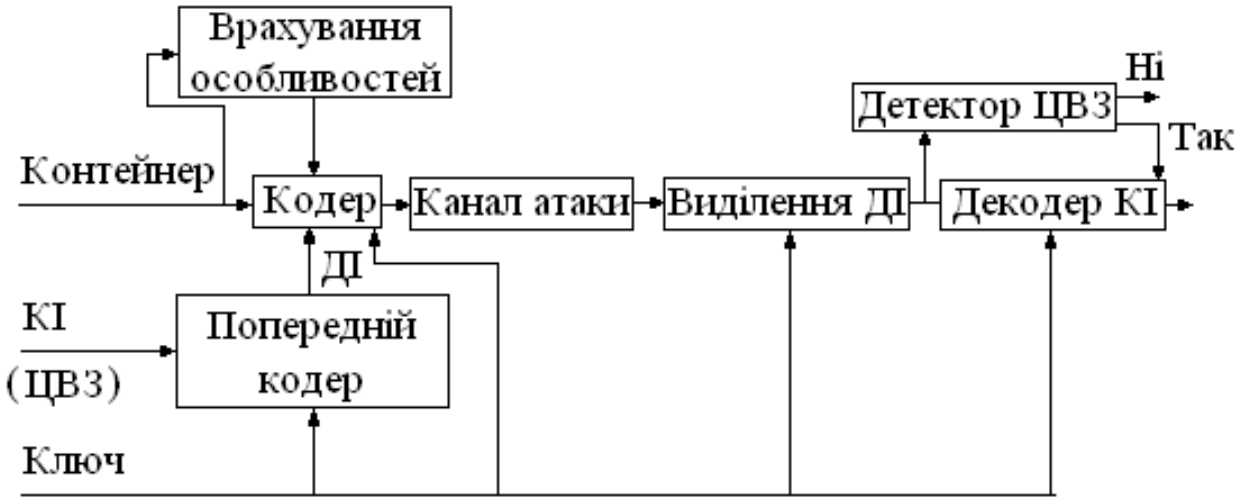

Рисунок 1.1. — Основні елементи стеганосистеми

Контейнер – будь-яка несекретні дані, які використовуються для приховування повідомлення. Якщо контейнер містить повідомлення, його

називають заповненим або стеганоповідомленням (СП), інакше пустим [10,11]. У комп'ютерній стеганографії як контейнер використовують різні відцифровані дані: цифрове зображення (ЦЗ), звукову послідовність, відеопослідовність, а також текстові та інші електронні документи. Виокремлюють два типи контейнерів: потоковий та фіксований [10,11].

Повідомлення – секретна інформація, наявність якої в контейнері необхідно приховати [10,11]. Секретну інформації перед процесом занурення перетворюють у необхідний для цього вид, зазвичай у бінарну послідовність з 0 та 1, яка має назву додаткова інформація (ДІ). Пристрій, призначений для цього у стеганосистемі має назву прекодер.

Саме на цьому кроці можливе застосування криптографії, що дозволяє не лише забезпечити додатковий захист, а й скоротити розмір переданого повідомлення [14].

Ключ – секретна інформація відома тільки законному користувачеві, яка визначає конкретний вид алгоритму приховування [7].

1.2 Огляд стеганоалгоритмів, стійких до атак проти вбудованого повідомлення

До будь-якого стеганографічного алгоритму на ряду з такими вимогами як забезпечення надійності сприйняття стеганоповідомлення та достатня пропускна спроможність прихованого каналу зв'язку, висувається одна з основних вимог для забезпечення ефективного декодування секретного повідомлення – стійкість до атак проти вбудованого повідомлення [15, 16.]. Прикладами таких атак можуть бути фільтрація, стиск зображень, додавання шуму, вирівнювання гістограми, зміна контрастності тощо [10]. Стійкість стеганографічного алгоритму визначається як нечутливість сформованого стеганоповідомлення до збурних дій.

Робота в даному напрямку ведеться в даний момент дуже активно, при цьому для вбудови додаткової інформації використовуються різні області контейнера: просторова, області дискретного косинусного перетворення, області

дискретного перетворення Фур'є, області дискретного вейвлет-перетворення [17, 18].

Так в [19] був розроблений стеганографічний метод і реалізуючий його ефективний поліноміальний стеганоалгоритм, в якому в стеганоперетвореннi задіюється просторова область ЦЗ-контейнера після попереднього розбиття його матриці на блоки, що не перетинаються. Однак недоліком методу є негарантоване збереження надійності сприйняття формованого стеганоповідомлення в тому випадку, коли ЦЗ-контейнер має значні по розмірі фонові області. Усуненню цього недоліку присвячена робота [20], в якій запропонована модифікація методу, що досягається за рахунок зменшення стрибка функції яскравості пікселів на границі блоків матриці ЦЗ-контейнера при вбудові ДІ шляхом зміни виду матриці збурення блоку контейнера при стеганоперетвореннi.

В [21] пропонується стійка до збурних дій схема вбудови ДІ для забезпечення захисту авторських прав. Тут вбудова біт ДІ відбувається в синю компоненту кольорового ЦЗ (в кольоровій схемі RGB) або в компоненту яскравості (в кольоровій схемі YUV) в області дискретного вейвлет-перетворення. Для забезпечення стійкості стеганоалгоритму кожний біт ДІ вбудовується в три позиції виділеної матриці контейнера, які визначаються секретним ключем.

Актуальність таких алгоритмів визначається певними областями їх застосування з передбачуваними збурними діями. Прикладом таких алгоритмів є стеганоалгоритм з [22], заснований на теоремі лишків, та багато інших. Але проблема забезпечення стійкості стеганоалгоритмів до атак проти вбудованого повідомлення не є повною мірою вирішеною, залишається актуальною, оскільки більшість з існуючих методів орієнтована на конкретні збурні дії, стаючи неспроможними в умовах атак, що відрізняються від передбачуваних. Головною причиною цього є обмеженість математичних базисів існуючих методів, їх орієнтованість на конкретні атаки проти вбудованого повідомлення.

Протягом довгого часу вважалося, що для забезпечення стійкості стеганографічних методів і алгоритмів до збурних дій кращою для вбудови ДІ є частотна область зображення [23,24]. Велика частина сучасних розроблюваних

стійких стеганоалгоритмів працюють в області дискретного косинусного перетворення та перетворення Фурьє. Актуальність алгоритмів, що працюють з цією областю визначається простотою забезпечення вимоги стійкості: використовуючи для занурення ДІ низькочастотні коефіцієнти ЦЗ, виділити які у частотній області розкладання не представляє труднощів.

Одним з найпоширеніших стеганографічних методів, що вбудовує додаткову інформацію у частотну область та позиціонується як стійкий до стиснення, є метод Коха і Жао. Для стеганоперетворення обирається два середньочастотні коефіцієнти дискретного косинусного перетворення блоку матриці ЦЗ. Вбудовування ДІ відбувається шляхом кореляції значень обраних коефіцієнтів. Однак метод залишається ефективним лише для стиснення з високим коефіцієнтом якості.

Як показано у [25], забезпечення стійкості стаганоалгоритму не залежить від обраної для вбудови ДІ області зображення. Будь-які зміни, що відбуваються при зануренні ДІ в будь-якій області контейнера (просторової, області перетворення) однозначно відображаються у вигляді певних змін в інших областях (перетворення, просторової), що призводять до тих же результатів, що стосуються стійкості СП, тому частотна область не має переваг в порівнянні з будь-якою іншою областю ЦЗ.

Незважаючи на те, що стійкість стеганографічного методу не залежить від області занурення ДІ, але формальні достатні умови забезпечення стійкості стеганографічного алгоритму до збурних дії, визначені в [26, 15] використовують область сингулярного розкладання матриці контейнера. Тому в роботі розглядається саме ця область для стеганоперетворення.

Зробивши аналіз літературних джерел по темі кваліфікаційної роботи можна зробити наступні висновки:

– стеганографія була та залишається одним з основних напрямків захисту інформації;

– серед вимог, що висуваються до стеганографічних алгоритмів, одною з основних є вимога стійкості до атак проти вбудованого повідомлення;

– найбільш використовуваною областю ЦЗ-контейнера при організації стеганоперетворення, стійкого до атак проти вбудованого повідомлення, у тому числі атаки стиском, залишається частотна область, хоча не має реальних переваг перед будь-якою іншою областю ЦЗ-контейнера;

– задача розробки стеганографічних алгоритмів, стійких до атак проти вбудованого повідомлення остаточно не вирішена, адже більшість алгоритмів орієнтовані на конкретні збурні дії, їх ефективність залишається такою, що може бути збільшена шляхом застосування нових математичних базисів.

2 РОЗРОБКА СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ, СТІЙКОГО ДО АТАКИ ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

2.1 Визначення області цифрового зображення для стеганоперетворення, стійкого до атаки стиском

У якості формального представлення контейнера розглядається одна матриця, що відповідає одній кольоровій компоненті ЦЗ, а ДІ – сформована випадковим чином бітова послідовність: $p_1, p_2, \dots, p_t,\ p_i \in \{0,1\}, i = \overline{1,t}$.

Властивості стеганоалгоритмів, в тому числі і їх стійкість до збурних дії, не визначається областю контейнера, яку використовують для занурення ДІ, а як показано в [25,26] залежить від величин та локалізації збурень повного набору формальних параметрів, які характеризують контейнер, що відбувались при стеганоперетворенні. [27]. Тому першою з задач для розробки алгоритму, що буде стійким до атак проти вбудованого повідомлення, в тому числі атаки стиском, буде аналіз повного набору параметрів та виявлення тих, що будуть найменш чутливими до збурень.

Відповідно до [28], будь-яке стеганоперетворення матриці контейнеру може бути представлено у вигляді:

$$\bar{F} = F + \Delta F, \tag{2.1}$$

де F – матриця ЦЗ-контейнер;

ΔF – матриця збурення контейнера в наслідок стеганоперетворення.

У якості повного набору формальних параметрів, однозначно визначаючих стан контейнера можна розглядати один з таких наборів – сукупність сингулярних чисел (СНЧ) та сингулярних векторів (СНВ) відповідних матриць, що однозначно визначаються нормальним сингулярним розкладанням [28]:

$$F = U\Sigma V^T, \tag{2.2}$$

де U, V – ортогональні $n \times n$ матриці, стовпці матриці U – ліві СНВ, лексикографічно додатні, стовпці матриці V – праві СНВ матриці F;

$\Sigma = diag(\sigma_1, \dots, \sigma_n), \sigma_1 \geq \cdots \geq \sigma_n \geq 0$ – матриця СНЧ.

Під нормальним сингулярним розкладанням розглядають таке, для якого стовпці матриці U лексикографічно додатні, тобто перша його ненульова компонента є додатною [28].

Будь-яке перетворення (атака стиском або накладання шумів), що відбудеться з контейнером збурить її матрицю, і як наслідок збурить відповідні СНЧ та СНВ [28].

Для вбудовування ДІ доцільно використовувати ті параметри нормального сингулярного розкладання, що будуть найменш чутливими до збурень, що можуть бути викликані атаками проти вбудованого повідомлення, в тому числі збереженням ЦЗ-контейнеру після стеганоперетворення у формат з втратами або накладання шуму.

Чутливість СНВ будь-якої матриці різна відповідно до співвідношення [27]:

$$\frac{1}{2}\sin 2\theta_i \leq \frac{\|\Delta F\|_2}{svdgap(i, F + \Delta F)}, \; svdgap(i, F + \Delta F) \neq 0 \qquad (2.3)$$

де θ_i – кут між відповідними вихідними та збуреними сингулярними векторами u_i та $\overline{u_i}$;

ΔB – матриця збурених блоків B;

$\|\cdot\|_2$ – спектральна матрична норма;

svdgap(i, B) – відокремленість СНЧ σ_i матриці B, що визначається як:

$$svdgap(i, F) = \min_{i \neq j} |\sigma_j - \sigma_i| \qquad (2.4)$$

Відокремленість СНЧ, що відповідає збуренням СНВ матриці контейнеру, є мірою чутливості отриманого СП до збурних дій [26].

Відповідно до [15] збурення СНЧ порівняні зі збуренням даних ΔF, це означає, що СНЧ матриці, на відміну від СНВ, є добре обумовленими, тобто нечутливими до збурних дії відповідно до співвідношення [26]:

$$\max_{1\le j\le N} |\sigma_j(F) - \sigma_j(F + \Delta F)| \le \|\Delta F\|_2 , \qquad (2.5)$$

де ΔF – матриця збурень F;

$\|\cdot\|_2$ – спектральна матрична норма.

Використання області сингулярного розкладання матриці (блоків матриці ЦЗ) для стеганоперетворення дозволяє досягти необхідних властивостей алгоритму шляхом визначення збурень повного набору параметрів при зануренні ДІ та їх корегування змінами параметрів алгоритму.

Формальні достатні умови стійкості стеганографічного методу до стиску з втратами, що були отримані та сформульовані у [15], які враховують специфіку збурень СНЧ блоків матриці забезпечують стійкість до атак проти вбудованого повідомлення в цілому та використовуються при розробці стеганографічного методу.

Основною умовою для збереження стійкості є перевищення сукупного результату збурень найбільших СНЧ, які зазнає блок ЦЗ при зануренні ДІ у порівнянні зі збуреннями, що можуть бути викликані в результаті атаки проти вбудованого повідомлення.

Як правило, максимальне СНЧ σ_1 блоку ЦЗ значно відрізняється від всіх наступних, тим самим маючи максимальну відокремленість, яка значно перевершує відокремленості $\sigma_2, \dots, \sigma_l$, тобто $\sigma_1 \ge \sigma_2 \ge \dots \ge \sigma_l \ge 0$, значення яких представлені у таблиці 2.1 та 2.2 для різних за розміром блоків матриці ЦЗ. Для блоків оригінальних ЦЗ останнє співвідношення можна уточнити [30]:

$$\sigma_1 \gg \sigma_2 \ge \dots \ge \sigma_l \ge 0 \qquad (2.6)$$

Таблиця 2.1 – Середнє по зображенню величина відокремленості СНЧ 4×4-блоків

№ ЦЗ	Середнє значення відокремленості			
	$i = 1$	$i = 2$	$i = 3$	$i = 4$
1	581,762	2,046	0,391	0,264
2	274,759	12,783	3,298	0,581
3	144,647	3,123	0,846	0,334
4	361,490	9,678	3,162	0,447
5	766,897	9,150	4,620	0,679
Ср.зн-я (100 ЦЗ)	336,599	6,228	2,026	0,312

У таблиці 2.1 та 2.2 приведені середні по зображенню величини відокремленості СНЧ для блоків 4×4 та 8×8 відповідно. Очевидно, що відокремленість СНЧ не залежить від розміру блоку та співвідношення (2.6) виконується як для блоків 4×4 так і для 8×8.

Таблиця 2.2 – Середнє по зображенню величина відокремленості СНЧ 8×8-блоків

№ ЦЗ	Середнє значення відокремленості							
	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$	$i = 7$	$i = 8$
1	828,5821	9,6204	3,7495	1,0735	0,5121	0,2983	0,2023	0,0807
2	42,1862	1,8959	0,5927	0,5062	0,2960	0,2298	0,1784	0,0705
3	1701,2949	7,4602	2,3077	0,6433	0,2678	0,1764	0,1163	0,0455
4	483,5682	9,7481	3,1149	0,9461	0,4786	0,3722	0,3010	0,1258
5	691,8637	9,3863	3,3480	0,7915	0,3297	0,2481	0,1961	0,0778
Ср.зн-я(100 ЦЗ)	663,9764	15,8357	7,4747	2,9963	1,3349	0,6341	0,3670	0,1338

Співвідношення (2.6) приводить до того, що для більшості блоків оригінального ЦЗ справедливе наступне [31]:

$$\angle(\sigma, e_1) \approx 0\,, \tag{2.7}$$

де $\angle(\sigma, e_1)$ – величина кута між векторами СНЧ $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_l)^T$ та $e_1 = (1, 0\,, \dots, 0)^T \in R^l$ – першим вектором стандартного базису простору R^l. Саме ця характеристика використовується для вбудовування та декодування ДІ.

2.2 Стеганографічний метод, стійкий до атаки проти вбудованого повідомлення

Опираючись на характерні особливості співвідношення куту між вектором СНЧ та першим вектором стандартного базису (2.7) для блоку оригінального ЦЗ, наведеному в попередньому пункті, було розроблено стеганографічний метод.

У якості контейнеру можливе використання кольорових зображень та зображень у градаціях сірого. При використанні кольорового ЦЗ вбудовування ДІ буде проводитись в одну з матриць R, G або B, для більшої ймовірності забезпечення надійності сприйняття. У якості ДІ розглядається послідовність отримана попереднім переведенням прихованого повідомлення у бінарний код p_1, $p_2, \dots, p_t$, де $p_i \in \{0,1\}$, $i = 1, 2, \dots, t$. У кожний блок матриці вбудовується 1 біт ДІ. Виходячи з потужності алфавіту, що дорівнює двом, необхідно передбачити два можливих варіанти перетворення блоку. Тому кожному $l*l$-блоку B з елементами $b_{ij}, i, j = 1, \dots, l$, ставимо у відповідність дві симетричні $l \times l$ – матриці B_v і B_n за наступним правилом:

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1l} \\ b_{21} & b_{22} & \dots & b_{2l} \\ \dots & \dots & \dots & \dots \\ b_{l1} & b_{l2} & \dots & b_{ll} \end{pmatrix} \rightarrow B_V = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1l} \\ b_{12} & b_{22} & \dots & b_{2l} \\ \dots & \dots & \dots & \dots \\ b_{1l} & b_{2l} & \dots & b_{ll} \end{pmatrix}, \quad B_N = \begin{pmatrix} b_{11} & b_{21} & \dots & b_{l1} \\ b_{21} & b_{22} & \dots & b_{l2} \\ \dots & \dots & \dots & \dots \\ b_{l1} & b_{l2} & \dots & b_{ll} \end{pmatrix}, \tag{2.8}$$

отримані відображенням верхнього (для B_v) та нижнього (для B_n) трикутника блоку B відносно головної діагоналі.

Основні кроки методу мають наступний вигляд.

Вбудова ДІ.

Крок 1. Матрицю F ЦЗ-контейнера розбити стандартним чином на $l \times l$-блоки, що не перетинаються.

Крок 2 *(вбудова ДІ)*. Для кожного $l \times l$-блоку B матриці контейнера, що бере участь у стеганоперетворенні (порядок використання блоків є частиною секретного ключа) для вбудови p_{ij} - чергового біта ДІ, робити:

2.1. Сформувати матриці B_V і B_N відповідно до (2.8).

2.2. Для B_V і B_N визначити вектори СНЧ: $\sigma(B_V) = (\sigma_1(B_V),...,\sigma_l(B_V))^T$ і $\sigma(B_N) = (\sigma_1(B_N),...,\sigma_l(B_N))^T$ відповідно шляхом нормальних сингулярних розкладань (2.2): $B_V = U_V \Sigma_V V_V^T$, $B_N = U_N \Sigma_N V_N^T$. При вбудові біта ДІ зміни будуть вноситися в одну з матриць B_V, B_N.

2.3. *Якщо*

$$p_{ij} = 0,$$

то

2.3.1. Забезпечити умову:

$$\angle(\sigma(B_N), e_1) > \angle(\sigma(B_V), e_1), \tag{2.9}$$

збурюючи СНЧ B_N. Результат: збурена матриця СНЧ $\overline{\Sigma}_N$.

2.3.2. Сформувати збурену матрицю $\overline{B}_N$ з елементами $\overline{b}_{ij}^{(N)}, i, j = \overline{1,l}$: $\overline{B}_N = U_N \overline{\Sigma}_N V_N^T$.

2.3.3. Сформувати блок $\overline{B}$ стеганоповідомлення, який відповідає блоку B контейнера, в вигляді:

$$\overline{B} = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1l} \\ \overline{b}_{21}{}^{(N)} & b_{22} & \dots & b_{2l} \\ \dots & \dots & \dots & \dots \\ \overline{b}_{l1}{}^{(N)} & \overline{b}_{l2}{}^{(N)} & \dots & b_{ll} \end{pmatrix} \tag{2.10}$$

інакше

2.3.1. Забезпечити умову:

$$\angle(\sigma(B_N), e_1) < \angle(\sigma(B_V), e_1), \tag{2.11}$$

збурюючи СНЧ B_V. Результат: збурена матриця СНЧ $\overline{\Sigma}_V$.

2.3.2. Сформувати збурену матрицю $\overline{B}_V$ з елементами $\overline{b}_{ij}{}^{(V)}, i, j = \overline{1,l}$: $\overline{B}_V = U_V \overline{\Sigma}_V V_V{}^T$.

2.3.3. Сформувати блок $\overline{B}$ стеганоповідомлення, який відповідає блоку B контейнера, в вигляді:

$$\overline{B} = \begin{pmatrix} b_{11} & \overline{b}_{12}{}^{(V)} & \dots & \overline{b}_{1l}{}^{(V)} \\ b_{21} & b_{22} & \dots & \overline{b}_{2l}{}^{(V)} \\ \dots & \dots & \dots & \dots \\ b_{l1} & b_{l2} & \dots & b_{ll} \end{pmatrix} \tag{2.12}$$

Крок 3. З урахуванням змінених у результаті стеганоперетворення блоків матриці ЦЗ сформувати матрицю $\overline{F}$ стеганоповідомлення. Процес вбудови ДІ завершено.

Нехай $\overline{\overline{F}}$ - матриця стеганоповідомлення, яка, в загальному випадку, у результаті атак проти вбудованого повідомлення може зазнати змін та бути відмінною від $\overline{F}$.

Декодування ДІ.

Крок 1. Матрицю $\overline{\overline{F}}$ ЦЗ-стеганоповідомлення розбити стандартним чином на $l \times l$-блоки, що не перетинаються.

Крок 2 *(декодування ДІ)*. Для кожного $l \times l$-блоку $\overline{\overline{B}}$ матриці стеганоповідомлення, який брав участь в стеганоперетвореній (порядок блоків є частиною секретного ключа), робити:

2.1. Для блока $\overline{\overline{B}}$ сформувати матриці $\overline{\overline{B}}_V$ і $\overline{\overline{B}}_N$ відповідно до (4).

2.2. Для $\overline{\overline{B}}_V$ і $\overline{\overline{B}}_N$ визначити вектори СНЧ: $\overline{\overline{\sigma}}(B_V) = \left(\overline{\overline{\sigma}}_1(B_V),...,\overline{\overline{\sigma}}_l(B_V)\right)^T$ і $\overline{\overline{\sigma}}(B_N) = \left(\overline{\overline{\sigma}}_1(B_N),...,\overline{\overline{\sigma}}_l(B_N)\right)^T$. Нехай $\overline{\overline{p}}_{ij}$ - черговий біт ДІ, що декодується з чергового блоку $\overline{\overline{B}}$ стеганоповідомлення.

2.3. Визначити значення кутів $\angle\left(\overline{\overline{\sigma}}(B_N), e_1\right)$, $\angle\left(\overline{\overline{\sigma}}(B_V), e_1\right)$.

2.4. *Якщо*

$$\angle\left(\overline{\overline{\sigma}}(B_N), e_1\right) < \angle\left(\overline{\overline{\sigma}}(B_V), e_1\right),$$

то

$$\overline{\overline{p}}_{ij} = 1,$$

інакше

$$\overline{\overline{p}}_{ij} = 0.$$

Основним аспектом при розробці алгоритму було забезпечення умови (2.9) або (2.11) при зануренні ДІ. Оскільки, величина кута $\angle(\sigma, e_1)$ залежить від того, наскільки відрізняються між собою перше та друге СНЧ, адже наступні СНЧ відрізняються одне від одного значно менше, то змінюючи значення лише першого та другого СНЧ, зменшуючи величину між ними, можна корегувати величину кута. Уточнимо крок 2.3.1 (вбудова ДІ) наступним чином:

2.3.1. Забезпечити умову: $\angle(\sigma(B_N), e_1) > \angle(\sigma(B_V), e_1)$ $\left(\angle(\sigma(B_N), e_1) < \angle(\sigma(B_V), e_1)\right)$, збурюючи СНЧ B_N (B_V):

$$\sigma_1(B_N) = \sigma_1(B_V) - T,\ \sigma_2(B_N) = \sigma_2(B_V) + T \quad \left(\sigma_1(B_V) = \sigma_1(B_N) - T,\ \sigma_2(B_V) = \sigma_2(B_N) + T\right), \quad (2.13)$$

де $T > 0$ - параметр, установлюваний експериментально. Результат: збурена матриця СНЧ $\bar{\Sigma}_N$ ($\bar{\Sigma}_V$).

Важливим моментом є те, що головна діагональ сформованого блоку $\bar{B}$ згідно (2.10) та (2.12) відповідає блоку B контейнера. Така діагональ залишається оригінальною для тієї з матриць B_V, B_N, яку вбудова біта ДІ не торкнулася, залишаючи кут у ній між нормованим вектором СНЧ і першим вектором стандартного базису відповідного простору близьким до нуля (тобто в оригінальному виді (2.7)), і ця ж діагональ є додатковим збуренням для матриці, шляхом зміни якої проводилося стеганоперетворення, додатково збурюючи кут $\angle(\sigma, e_1)$, що позитивно відбивається на ході декодування ДІ в процесі порівняння кутів $\angle\left(\bar{\bar{\sigma}}(B_N), e_1\right)$, $\angle\left(\bar{\bar{\sigma}}(B_V), e_1\right)$.

2.3 Вибір основних параметрів при розробці алгоритмічної реалізації методу

Одним з основних аспектів, що дозволяє досягти значної ефективності розроблюваного стеганоалгоритму, є вибір розміру блоків, на які розбивається матриця ЦЗ в процесі стеганоперетворення та декодування ДІ. Стандартним розміром блоку при розбитті матриці зображення вважається 8×8, адже саме на такі блоки розбивається матриця при стиску стандартом Jpeg. Вибір має проводитись таким чином, аби наближена рівність (2.7) виконувалась з найменшою похибкою.

Враховуючи це, розмір блоку було обрано, опираючись на [31], у якій результат обчислювального експерименту вказує, що з найбільшою точністю рівність (2.7) виконується для блоків розміром 4×4 оригінального ЦЗ, а тому виявити порушення цієї характеристики, що виникнуть у ході стеганоперетворення, при декодуванні ДІ буде легше саме для блоків 4×4.

Таким чином, в запропонованій в роботі алгоритмічній реалізації використовується значення параметру l=4.

При алгоритмічної реалізації стеганографічного методу необхідно було визначити значення параметру T. Це визначення повинно було забезпечити наступні вимоги:

1. Стійкість розроблюваного стеганоалгоритму до атак проти вбудованого повідомлення;

2. Збереження надійності прийняття формованого стеганоповідомлення.

Відповідно першій вимозі параметр T необхідно було робити як можна більшим, так як для принципової можливості декодування ДІ сукупний результат збурень, викликаний зануренням ДІ, повинен перевищувати збурення, що буде зазнавати стеганоповідомлення при атаках проти вбудованого повідомлення. Згідно з другою вимогою, параметр T повинен приймати як можна менше значення. Тому для забезпечення цих вимог, необхідно було знайти компроміс, який був досягнутий у ході обчислювального експерименту.

У загальному випадку збурення, що зазнає стеганоповідомлення при атаках проти вбудованого повідомлення, є незначними, адже результат цих дій має залишитись непомітним, інакше можуть виникнути видимі порушення надійності сприйняття, в наслідок чого атакуюча сторона може бути викрита.

В ході обчислювального експерименту, в якому були задіяні 100 ЦЗ, значення параметру T варіювалося в проміжку від 20 до 120. Порушення надійності сприйняття стеганоповідомлення встановлювалося за допомогою суб'єктивного ранжування, ефективність декодування оцінювалася кількістю (%) помилок при декодуванні $p_1, p_2, \ldots, p_t$, $p_i \in \{0,1\}$, $i = 1, 2, \ldots, t$.

В результаті експерименту значення параметру T обрано 90.

Таким чином було визначено розмір блоків, для розбиття матриці-контейнера, який дорівнює 4×4 пікселі, при якому ключова характеристика (2.7), яка використовується для вбудови та декодування ДІ, виконується найбільш точно. Експериментально було обрано параметр T, який задовольняє двом основним взаємовиключним вимогам, що висуваються до сучасних стеганографічних методів, велична якого дорівнює 90.

2.4 Аналіз ефективності стеганографічного алгоритму в умовах атаки проти вбудованого повідомлення

Для оцінки ефективності розробленого стеганографічного алгоритму було проведено обчислювальний експеримент, у якому було використано 100 ЦЗ у форматі без втрат (Tiff) – множина M_1 та 100 ЦЗ у форматі з втратами (Jpeg) – множина M_2, результати якого представлені у таблиці 2.3.

Таблиця 2.3 – Кількість помилок при декодування ДІ розробленим стеганоалгоритмом в умовах збереження стеганоповідомлення у формати з/без втрат (%)

Множина ЦЗ	Формат збереження ЦЗ після стеганоперетворення							
	Tiff	Jpeg						
		QF=60	*QF*=65	*QF*=70	*QF*=75	*QF*=80	*QF*=85	*QF*=90
M_1	0,0059	7,93	5,6	4,83	3,51	3,12	2,49	2,26
M_2	0,0052	6,89	4,39	3,67	2,35	2,1	1,76	1,51
Середнє значення	0,00555	7,41	4,995	4,25	2,93	2,61	2,125	1,885

З отриманих результатів можна зробити висновок, що правильність декодування вища для тих цифрових зображень, що вже зберігались у форматі з втратами. Це пояснюється тим, що при первісному збережені зображення у формат з втратами високочастотні, а при сильному стисненні і середньочастотні, коефіцієнти квантування дискретного косинусного перетворення вже піддались обнулінню. Тому при повторному збереженні частина коефіцієнтів квантування ДКП зазнають значно менші збурення, так як вже прийняли нульові значення.

Теоретичні основи розробленого алгоритму дозволяють забезпечити стійкість не лише до атаки стисненням, а й до інших атак проти вбудованого повідомлення. У таблиці 2.4 представлені результати експерименту за умовою накладання гауссовського та мультиплікативного шуму.

Таблиця 2.4 – Кількість помилок при декодуванні ДІ розробленим алгоритмом в умовах накладання шуму (%)

Множина ЦЗ	Шум, що накладається на СП		
	Гауссовський		Мультиплікативний, D=0.0001
	D=0.0001	D=0.001	
M_1	0,91	1,45	0,72
M_2	1,24	1,67	0,79
Середнє значення	1,075	1,56	0,755

Для порівняння ефективності розробленого стеганографічного алгоритму, який позначимо як *SA*, було використано наступні аналоги, що позиціонуються як стійкі до стиску, а саме: S_1 [32], S_2 [33], S_7 [17], SS_1 [34] (использующий амплитудную модуляцию), SS_2 [35] (использующий фазовую модуляцию), А2 [36] А3 [37]. В якості кількісної оцінки стійкості стеганоалгоритмів до збурень використовувався коефіцієнт кореляції для декодувати ДІ, який визначається відповідно до формули [38]: $NC = \sum_{i=1}^{t} p_i' \times \overline{p}_i' \Big/ t$, де $p_1, p_2, ..., p_t, p_i \in \{0,1\}, i = \overline{1,t}$ - ДІ, що занурена у контейнер; $p_i' = 1, \overline{p}_i' = 1$, якщо $p_i = 1, \overline{p}_i = 1$; $p_i' = -1, \overline{p}_i' = -1$, якщо $p_i = 0, \overline{p}_i = 0$. Результати порівняння розробленого алгоритму з існуючими, що позиціонуються як стійкі до атаки стиском в умовах стиску з різними коефіцієнтами якості представлено у таблиці 2.5.

Таблиця 2.5 – Значення NC для різних стеганоалгоритмів в умовах атаки стиском з різними коефіцієнтами якості *QF*

Стеганоалгоритм	*QF*(JPEG)				
	60	70	75	80	90
S_1	-	0.57	-	-	1
S_2	-	0.63	-	-	0.78
S_7	0.70	0.95	-	0.99	0.99

Продовження таблиці 2.5

SS_1	-	-	0.92	-	-
SS_2	-	-	0.95	-	-
$A2$	0.95	0.96	0.96	0.96	0.96
$A3$	0.94	0.94	0.94	0.94	0.94
SA	**0.862**	**0.927**	**0.953**	**0.958**	**0.97**

Виходячи з отриманих результатів, алгоритм по ефективності порівняний з існуючими аналогами в умовах атаки стиском. Як випливає з табл.3.3, найкращими з аналогів є S_7 і $A2$. Розроблений алгоритм SA незначно поступається S_7 при QF>60, але для QF=60 він на 23% перевищує ефективність S_7. В умовах QF=90 перевищує ефективність $A2$ на 1%. Крім того, розроблений алгоритм є стійким не тільки до атаки стиском, а взагалі до атак проти вбудованого повідомлення, що забезпечується його математичним базисом, а розглянуті аналоги – стеганоалгоритми, які позиціонуються як стійки до атаки саме стиском. Все це дозволяє говорити про підвищення ефективності прихованого каналу зв'язку при використанні для його створення розробленого алгоритму SA.

У розділі 2 були отримані наступні результати:

- обґрунтована доцільність використання області сингулярного розкладання блоків матриці ЦЗ-контейнера для організації стеганоперетворення;
- отримана умова, врахування якої забезпечує стійкість стеганоперетворення до атаки проти вбудованого повідомлення, яка була знайдена шляхом виділення з повного набору формальних параметрів, що визначають ЦЗ, тих, що є найменш чутливими до збурних дії. Цією умовою є близьке до нуля значення величини кута між вектором сингулярних чисел $l*l$-блоку, отриманого шляхом стандартної розбивки матриці зображення, та першим вектором стандартного базису простору R^l;

- на основі отриманих умов було розроблено стеганографічний метод, стійкий до атак проти вбудованого повідомлення, а також обрано та обґрунтовано параметри для алгоритмічної реалізації методу;
- розроблений алгоритм є стійким до атаки проти вбудованого повідомлення, що було підтверджено обчислювальним експериментом.
- кількість помилок при декодуванні ДІ в умовах атаки стиском з втратами при QF={60,65,70,75,80,85,90} становить від 1,885 (*QF=90*) до 7,41 (*QF*=60);
- розроблений алгоритм є стійким до накладання шуму: кількість помилок при декодуванні ДІ в умовах накладання гауссівського та мультиплікативного шумів, при D={0.001,0.0001} становить від 0,755% до 1,56%.
- розроблений алгоритм по ефективності є порівняним з сучасними аналогами в умовах атаки стиском: у порівнянні з сучасними аналогами, розроблений поступається при деяких *QF*, але показує кращий результат при інших (при *QF=60* має кращий результат за S_7 на 23%, а при *QF=90* перевищує ефективність на 1% $A2$). При цьому алгоритми, з якими проводилося порівняння, позиціонуються як стійкі до атаки стиском, а розроблений алгоритм є стійким до атак проти вбудованого повідомлення, що дозволяє сказати про досягнення мети та підвищення ефективності прихованого каналу зв’язку.

3 ОПИС ПРОГРАМНОГО ПРОДУКТУ

Реалізація методу має вигляд програмного продукту. Для початку роботи з ним користувачу необхідно запустити файл «diplom.exe», після чого на екрані з’явиться головне вікно інтерфейсу, яке представлено на рисунку 3.1. Фрагмент коду, що описує програмне забезпечення наведено у додатку А.

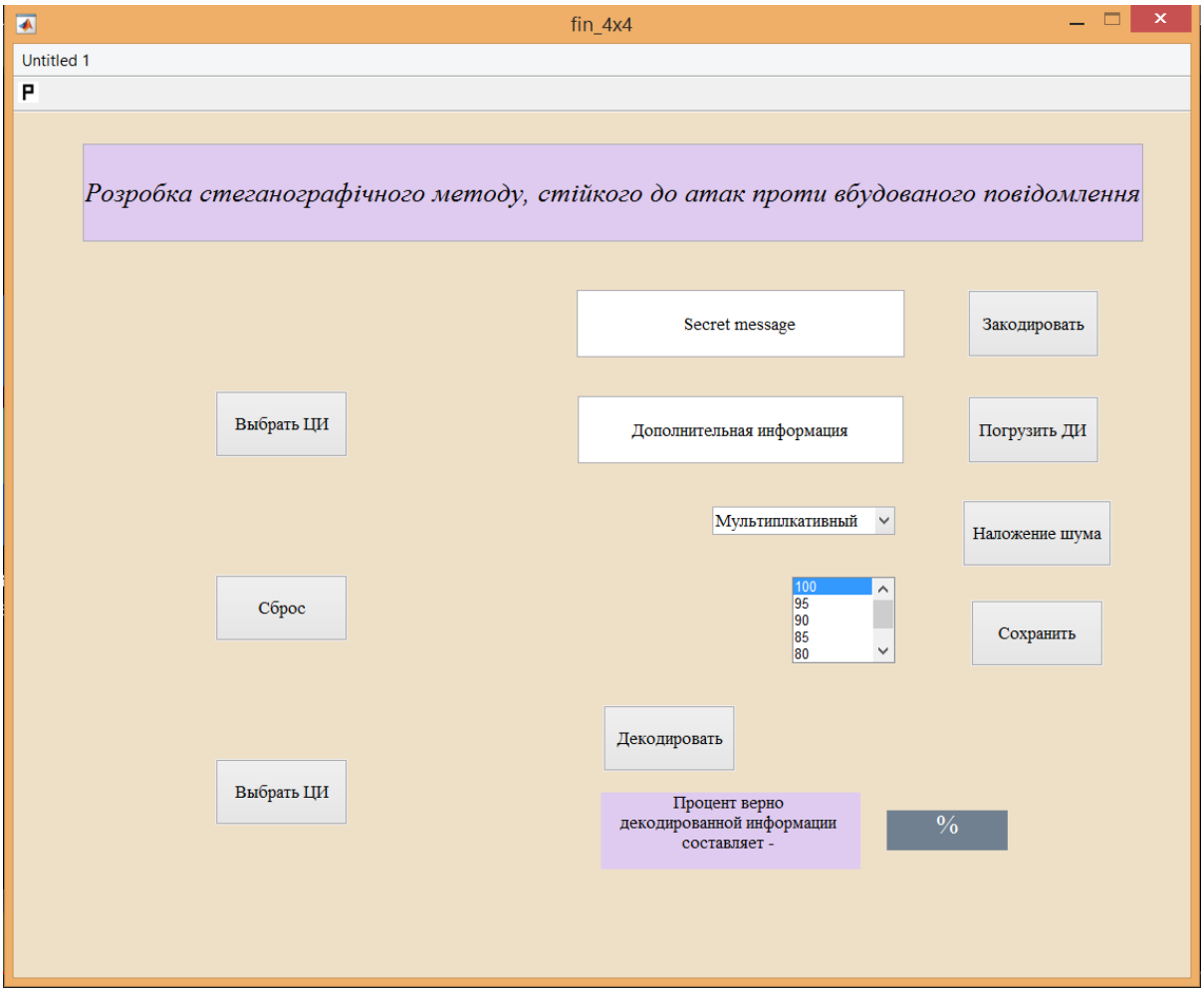

Рисунок 3.1 – Головне вікно програми

Першим кроком з якого починається занурення секретного повідомлення є вибір зображення, що виступає у ролі контейнера. Для цього необхідно натиснути на кнопку «Обрати зображення» та у вікні, що з’явиться обрати зображення-контейнер, у яке буде вбудована ДІ. Зображення з’явиться у верхньому полі, як показано на рисунку 3.2.

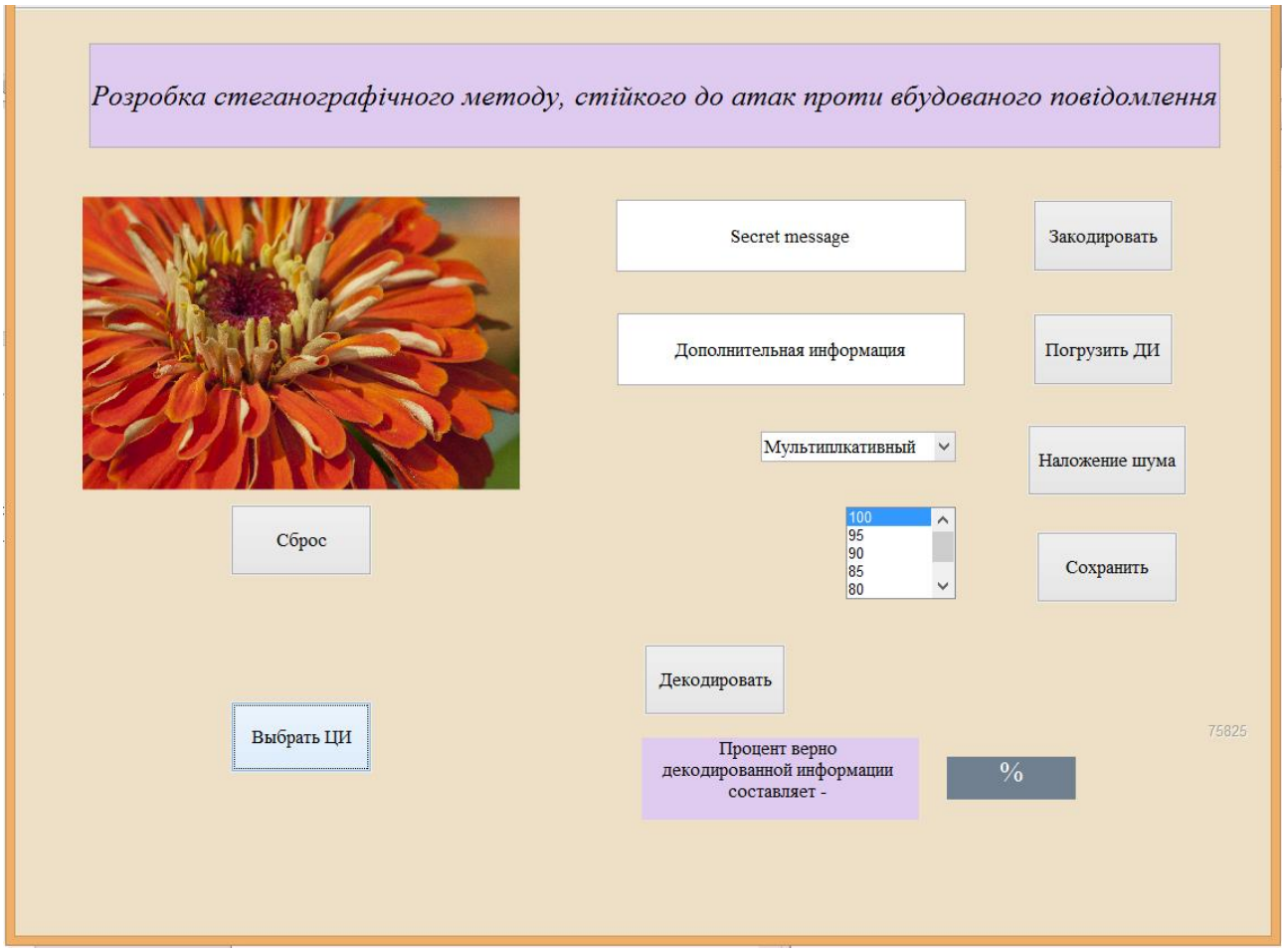

Рисунок 3.2 – Завантаження ЦЗ-контейнера

Наступним кроком є переведення секретного повідомлення, яке необхідно вбудувати у ЦЗ-контейнер, у додаткову інформацію, що у стегосистемі виконує прекодер. Для цього необхідно ввести необхідних текст у поле та натиснути кнопку «Закодувати». У програмному продукті встановлені перевірки. У разі якщо користувач не ввів секретне повідомлення та натиснув кнопку «Закодувати», він отримує попередження, що зображене на рисунку 3.3.

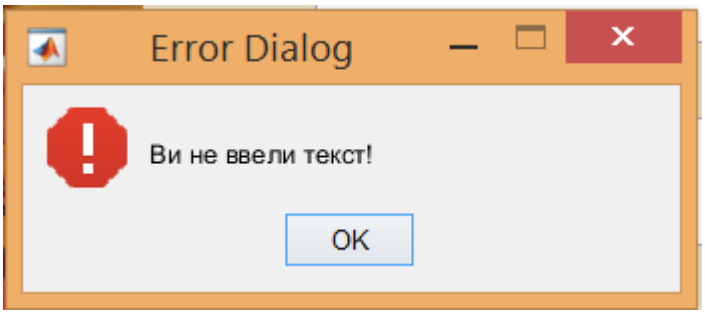

Рисунок 3.3 – Попередження про відсутність секретного повідомлення

Результат переведення секретного повідомлення у ДІ, а саме у бінарний код, представлено на рисунку 3.4.

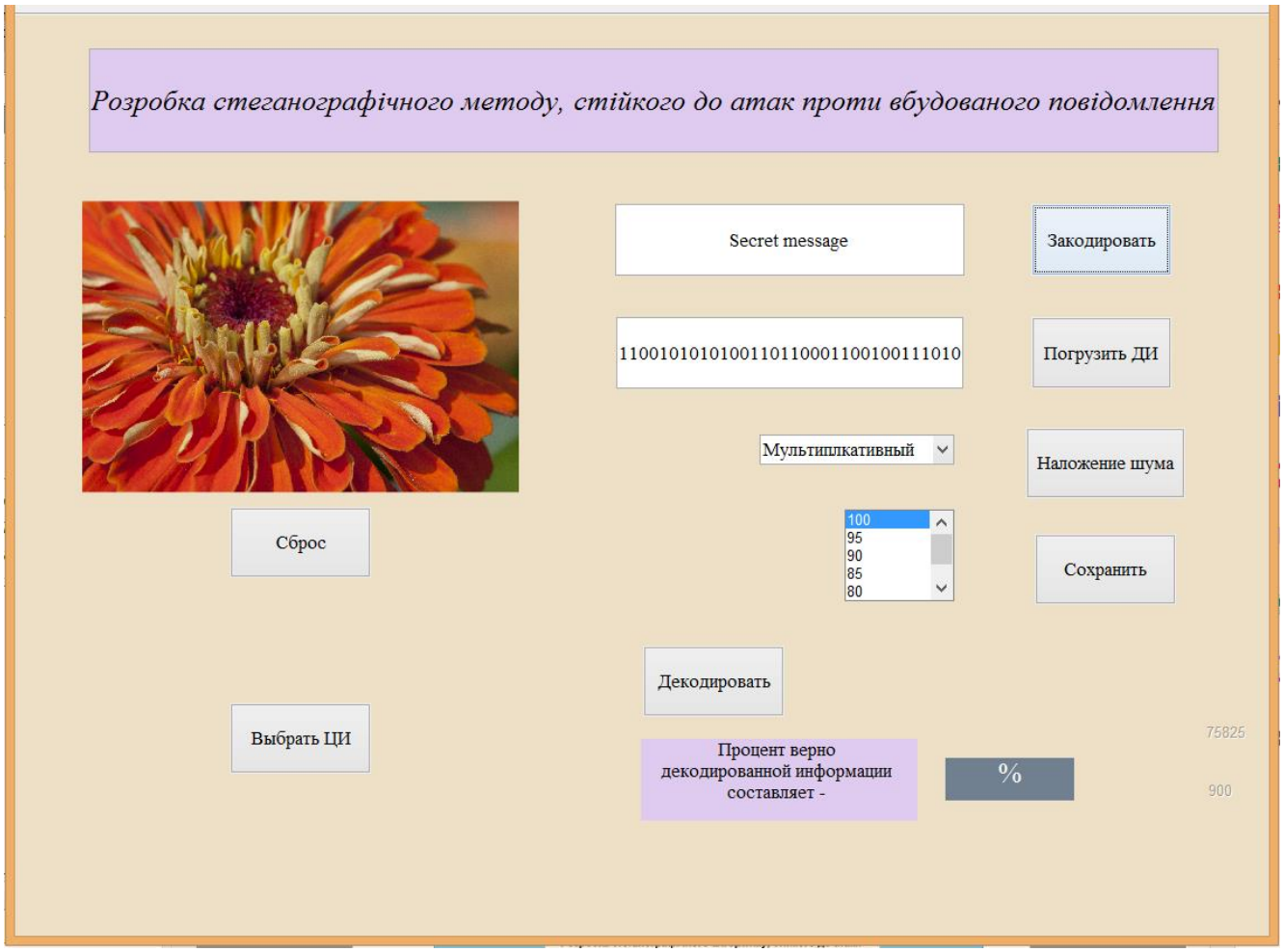

Рисунок 3.4 – Переведення секретного повідомлення у ДІ

Після натискання кнопки «Занурити текст» відбувається процес вбудовування ДІ шляхом виконання кроків, що описану у розділі 2. Після вбудови з’являється вікно з повідомленням про успішне занурення ДІ. А зображення з вбудованою інформацією заміняє те, що було обрано спочатку, для можливості оцінити надійність сприйняття. Результат роботи описаного кроку зображено на рисунку 3.5.

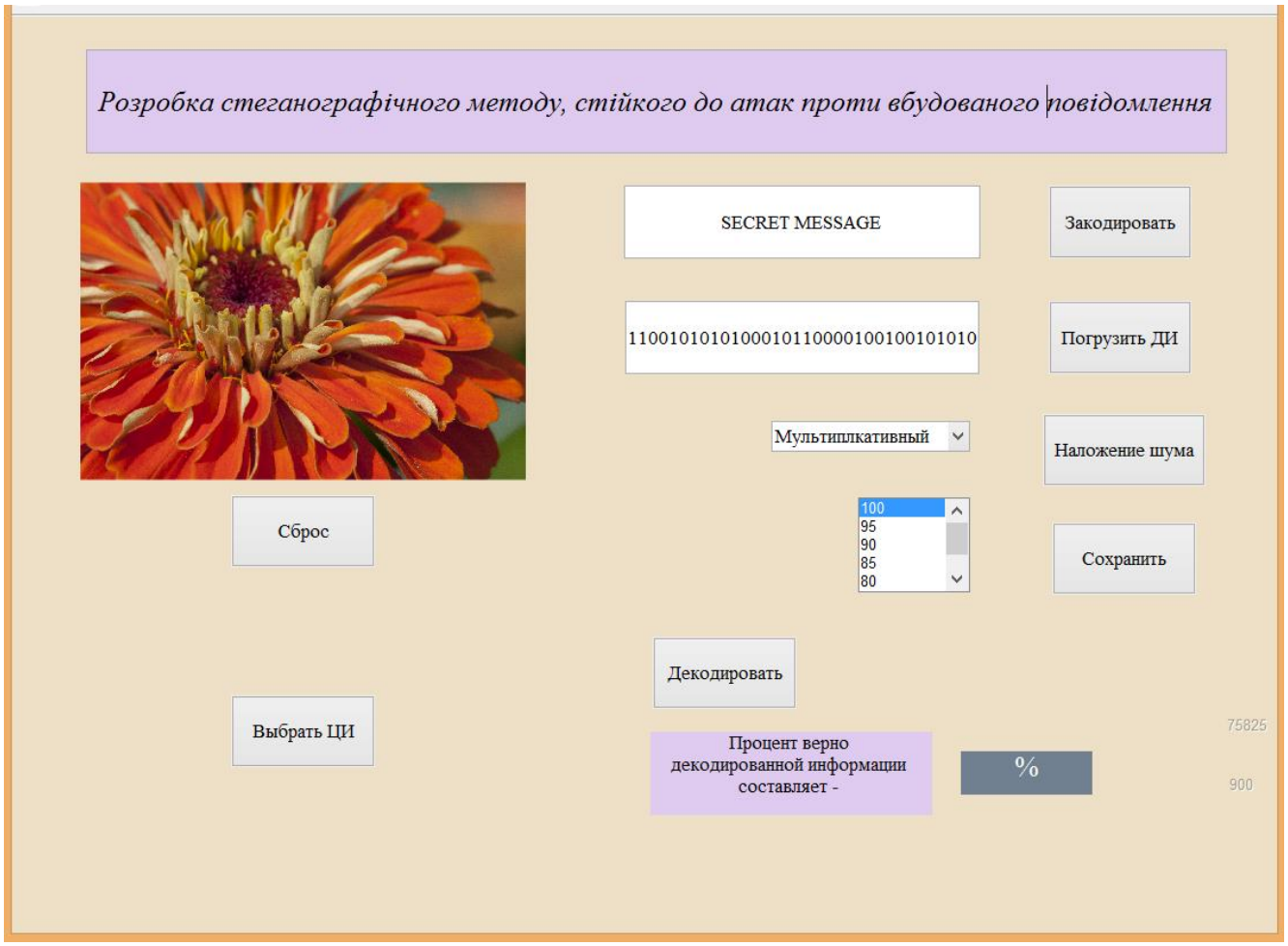

Рисунок 3.5 – Результат занурення ДІ

На цьому кроці також рахується кількість блоків, у які можна вбудувати додаткову інформацію, цей параметр залежить від розміру ЦЗ, та розмір переведеного секторного повідомлення. Якщо об’єм додаткової інформації перевищує максимальну кількість блоків, то користувач отримає сповіщення, що необхідно зменшити розмір секретного повідомлення, що зображено на рисунку 3.6.

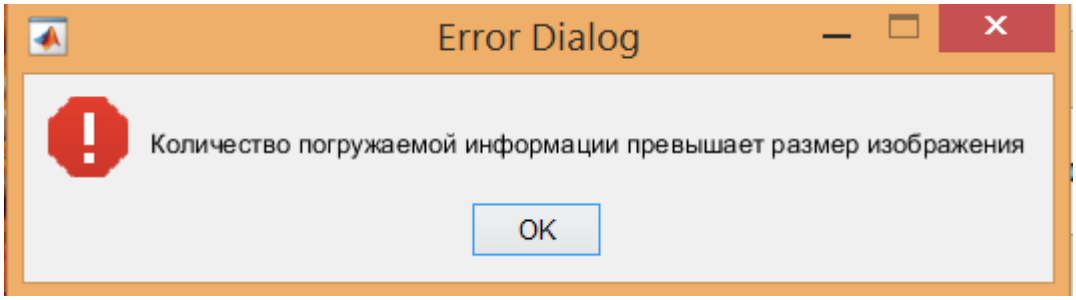

Рисунок 3.6 – Сповіщення про перевищення об’єму ДІ

Крім того, якщо користувач не обрав зображення-контейнер та намагається вбудувати ДІ, він також отримає попередження, що необхідно завантажити зображення.

Наступним кроком є збереження зображення, користувач має вибір коефіцієнтів якості для збереження у форматі Jpeg. Після натиснення кнопки «Зберегти» з'являється вікно, що представлене на рисунку 3.7, з можливістю ввести назву та обрати папку, у якій буде зберігатись стеганоповідомлення. Зображення у форматі без втрат зберігається автоматично у ту саму папку, яку обрав користувач з тим самим ім'ям, що ввів користувач. У разі успішного збереження програма повідомляє про це у вигляді діалогового вікна.

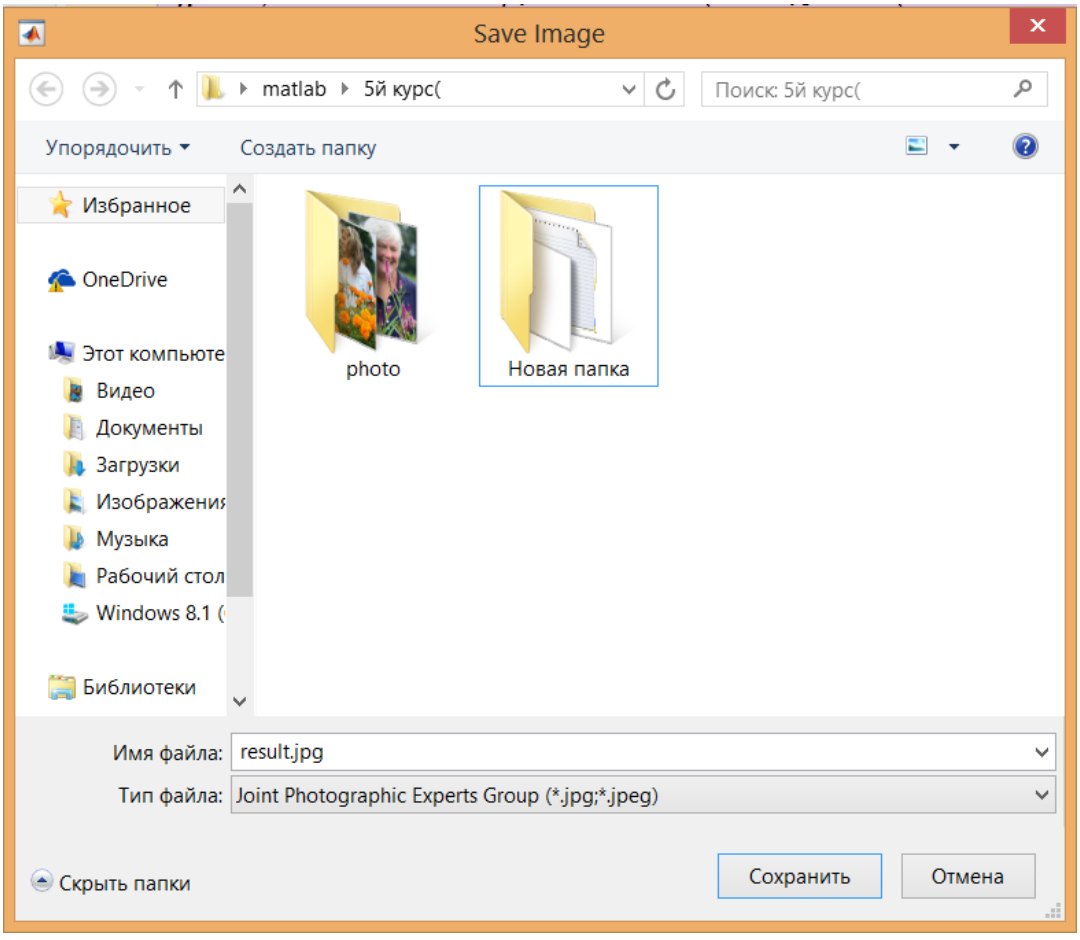

Рисунок 3.7 – Вікно збереження стеганоповідомлення

Далі йде етап декодування. Для цього необхідно обрати зображення, що було тільки що збережено, у вікні, яке з'явиться після натиснення кнопки «Обрати ЦЗ».

Після цього зображення з’явиться у відповідному місці, як показано на рисунку 3.8.

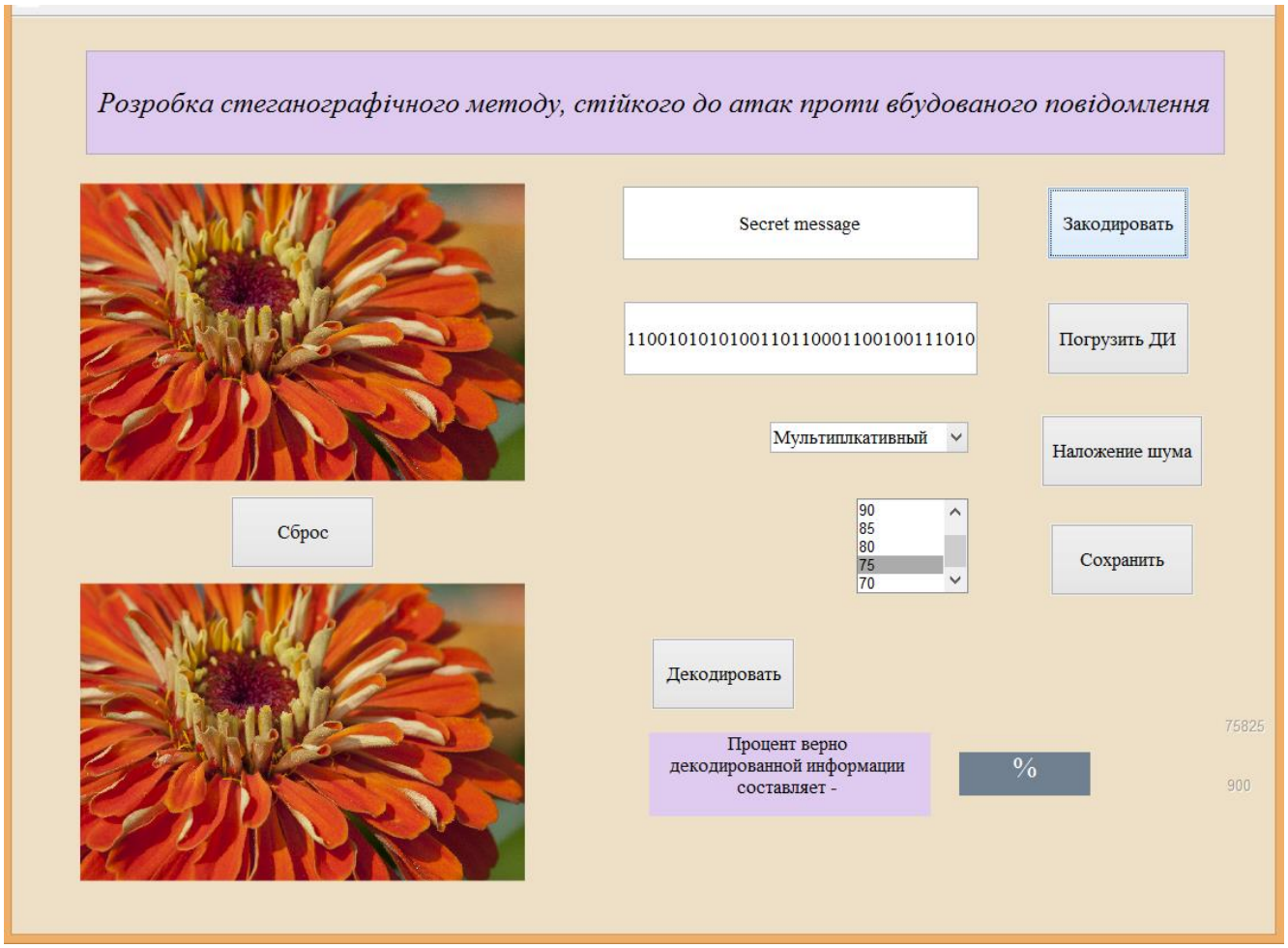

Рисунок 3.8 – Вибір зображення для декодування ДІ

Наступним кроком натискаємо кнопку «Декодувати», через декілька секунд у полі з’являється відсоток правильно декодованої інформації, як показано на рисунку 3.9.

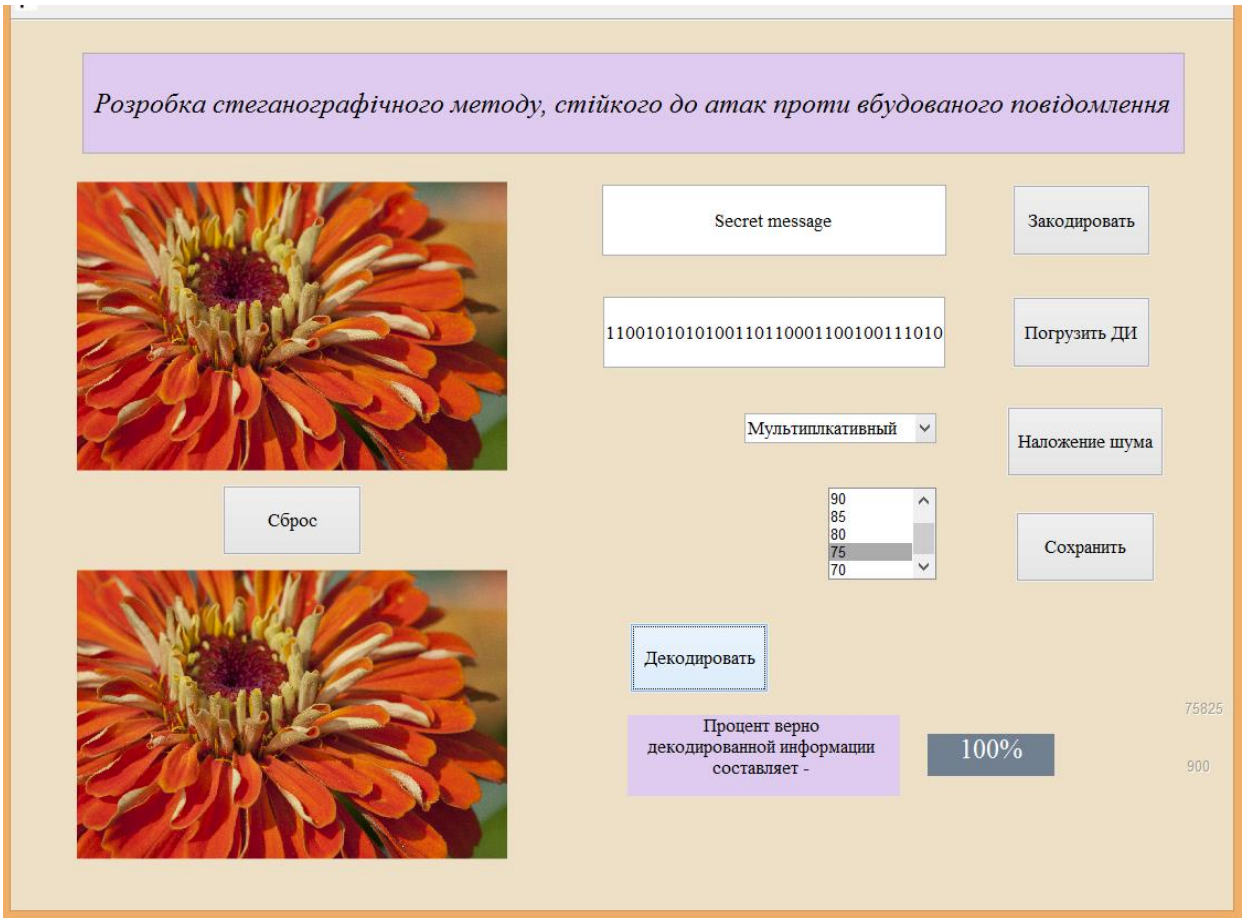

Рисунок 3.9 – Результат декодування додаткової інформації в умовах атаки стиском з втратами

Також у програмному інтерфейсі передбачено накладання шуму. Для цього перед кроком збереження стеганоповідомлення необхідно обрати вид: гауссовий чи мультиплікативний та параметр *D* для накладання шуму, далі натиснути кнопку «Накладання шуму» після чого зображення з шумом з’явиться у місці, де було обрано зображення для вбудови ДІ. Результат виконання цього кроку представлено на рисунку 3.10.

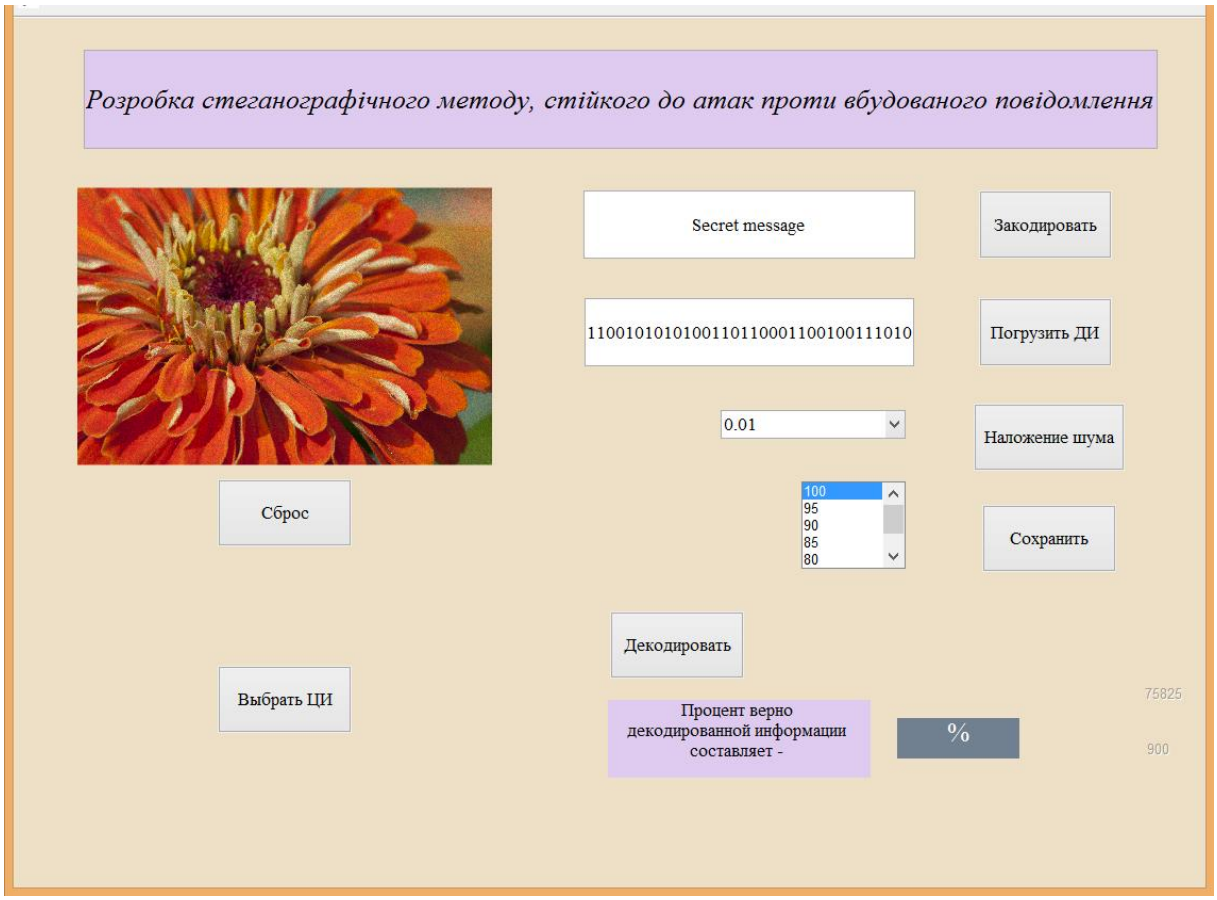

Рисунок 3.10 – Результат накладання шуму на стеганоповідомлення

Далі всі кроки відповідають декодуванню в умовах атаки стиском з втратами. Тобто користувач має зберегти зображення у необхідну папку та ввести назву зображення. Обрати щойно збережене стеганоповідомлення та натиснути кнопку «Декодувати», після чого у відповідному полі з’явиться результат декодування, який показано на рисунку 3.11

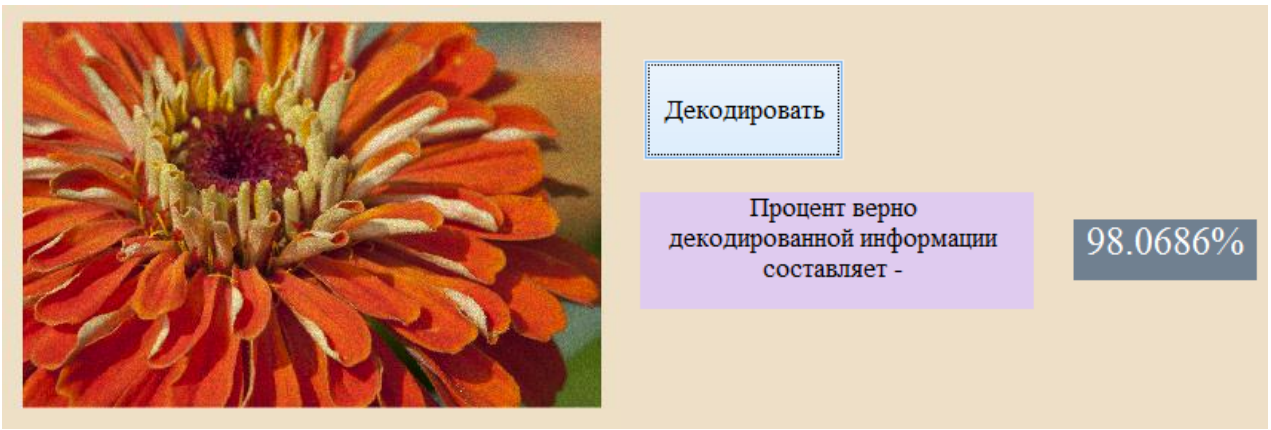

Рисунок 3.11 – Результат декодування ДІ в умовах накладання шуму

4 ОХОРОНА ПРАЦІ І БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯ

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

При розробці стеганографічного алгоритму, стійкого до атаки стиском використовується персональний комп'ютер. Тому предметом дослідження виступає комп'ютеризоване робоче місце, яке при недотримані умов експлуатації або неправильній організації може привести до погіршення стану здоров'я.

Велике значення для якості роботи мають антропометричні, фізичні і психологічні вимоги, розташування елементів комп'ютеризованого робочого місця, а також характер роботи.

Облаштування робочих місць, обладнаних ЕОМ, повинно забезпечувати [39]:

- належні умови освітлення приміщення і робочого місця, відсутність відблисків;
- оптимальні параметри мікроклімату (температура, відносна вологість, швидкість руху, рівень іонізації повітря);
- належні ергономічні характеристики основних елементів робочого місця;

Робоче місце працівника складається з робочого столу, стільця та персонального комп'ютера, який у свою чергу включає відеодисплейний термінал – далі ВДТ (монітор), системний блок, клавіатуру та комп'ютерну миш.

Приміщення, де розміщене комп'ютеризоване робоче місце знаходиться на першому поверсі будівлі, що споруджена за вимогами ДБН В.2.2-28:2010. Воно має наступні розміри: ширина – 5м, довжина – 4,3м, висота – 2,7м. Загальний об'єм складає 58,05м^3.

Приміщення має суміщене освітлення, що складається з природного – бокове одностороннє та штучного. До переваг природного освітлення можна віднести те, що воно сприятливо впливає на органи зору, стимулює фізіологічні процеси, але через відсутність стабільної освітленості у зв'язку зі змінами пір року та часу доби виникає необхідність у додатковому джерелі освітлення. Загальне освітлення здійснюється 4 люмінесцентними лампами (які мають близький до

денного спектральний склад світла), що розташовані на стелі, місцеве – світильниками, що розташовані безпосередньо на комп’ютеризованих робочих місцях. Все освітлення виповнялось відповідно до ДБН В.2.5-28-2006.

Головне завдання освітлення – створити найкращі умови для органів зору. Це завдання може бути вирішене тоді, коли виконуються такі вимоги до освітлення [40]:

- освітленість на робочому місці повинна відповідати характеру роботи органів зору, що визначається величиною найбільш дрібних предметів або їх частин, які необхідно відрізняти під час роботи, а також фоном та контрастом об'єкта розглядання і фону;
- необхідно забезпечувати достатньо рівномірне освітлення робочої поверхні, а також навколишнього простору;
- на робочій поверхні не повинно бути різких тіней;
- у полі зору не повинно бути прямої та відображеної блискучості, що може призвести до тимчасового осліплення;
- величина освітленості повинна бути постійною у часі.
- спектральний склад світла повинен по можливості забезпечувати правильну передачу кольору, тому штучне світло, що використовується на підприємствах, за своїм спектральним складом має наближатися до природного;
- освітлення повинно бути надійним, простим в експлуатації та економічним.

Кількість природного освітлення можна оцінити завдяки КПО (коефіцієнт природної освітленості). При наявності персонального комп’ютера на робочому місці КПО повинен дорівнювати 1,5% згідно з ДСанПіН 3.3.2-007-98 [39].

Крім природного освітлення, можна оцінити також й штучне. Його параметром є освітленість, яка повинна дорівнювати 750-300 лк, так як на робочому місці є комп’ютер.

Через те, що у приміщені розташовані механічні деталі, які є складовими персонального комп’ютера, їх рух може призвести до виникнення шуму.

Санітарні норми та заходи, що необхідно впровадити для зниження шкідливого впливу акустичних коливань мають відповідати ДСН 3.3.6.037-99.

Навіть при відносно незначних рівнях звуку, шум створює додаткове навантаження на нервову систему людини, що має негативний вплив на людей працюючих за ЕОМ. Шум не тільки заважає зосередиться, що веде до перенапруги, а тому і передчасної втоми, що викликає головний біль, але й збуджує нервову систему, підвищує тиск крові. Ці та інші порушення нормального функціонування організму людини можуть викликати негативні зміни в її емоційному стані, знижувати якість та безпеку праці, створює передумови до винекнення нещасних випадків.

Санітарно-гігієнічне нормування шумів на робочих місцях здійснюється згідно з ДСН 3.3.6.037. В основу гігієнічних норм покладені наступні принципи [39]:

- обмеження інтенсивності звукового тиску у межах октави;
- врахування характеру шуму;
- врахування особливостей трудової діяльності людини.

Для забезпечення допустимих рівнів шуму на робочих місцях слід застосовувати засоби звукопоглинання, вибір яких має обґрунтовуватись спеціальними інженерно-акустичними розрахунками [40].

Під час виконання робіт з персональним комп’ютером у виробничих приміщеннях значення характеристик вібрації на робочих місцях мають не перевищувати допустимі відповідно до СН 3044-84, ГОСТ 12.1.012-90, що становлять показник допустимих значень - 70 дБ [41]. Для запобігання розповсюдження вібрації застосовують амортизуючі прокладки.

Роботи за важкістю на основі загальних енерговитрат підрозділяються на 3 категорії (згідно ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»). Відповідно до цього користувачі персональних комп’ютерів виконують легку роботи, категорії Іа. Це використовується для визначення оптимальних параметрів мікроклімату на робочих місцях, які є одним з показників гігієнічної класифікації праці за умовами праці.

Параметри мікроклімату оснащених відеотерміналами, повинні відповідати вимогам пункту 2.4 СН 4088-86 "Санітарні норми мікроклімату виробничих приміщень".

Як параметр виробничого приміщення, мікроклімат впливає на теплообмін організму людини в цьому приміщені і, таким чином, визначає тепловий стан організму людини в процесі праці.

Мікрокліматичні умови виробничих приміщень визначаються поєднанням таких показників: температура повітря (°С), відносна вологість повітря (%), швидкість руху повітря (м/с), температура оточуючих людину поверхонь, інтенсивністю теплового (інфрачервоного) опромінення [39].

Оптимальні і допустимі параметри мікроклімату встановлюють залежно від загальних енерговитрат організму при виконанні робіт і періоду року.

Для категорії Іа у холодний період року, коли середньодобова температура повітря нижча +10 °С оптимальними параметрами робочої зони є наступні: температура повітря – 22 - 24 °С, відносна вологість – 40 - 60%, швидкість руху – 0,1 м/с; у теплий період року, коли середньодобова температура повітря вища +10 °С оптимальними параметрами є наступні: температура повітря – 23 - 25 °С, відносна вологість – 40 - 60 %, швидкість руху – 0,1 м/с.

Фактичні показники у приміщенні (тепла пора року) такі: температура повітря – 24 градусів С, відносна вологість – 45%, а швидкість руху повітря – 0,2 м/с. Виходячи з цього, фактичні показники відповідають нормативним значенням мікроклімату.

Задовольняючи нормальні умови мікроклімату виробничі приміщення повинні бути забезпечені опаленням у холодну пору року та вентиляцією у теплу, які мають відповідати вимогам СНиП 2.04.05-91 «Отопление, вентиляция и кондиционирование».

У виробничих приміщеннях, в яких не можна встановити допустимі величини мікроклімату через технологічні вимоги до виробничого процесу, технічну недосяжність або економічно обґрунтовану недоцільність передбачаються заходи

щодо захисту від можливого перегрівання та охолодження, відповідно до ДСН 3.3.6.042-99.

При роботі ВДТ персонального комп’ютера іонний склад повітря на робочому місці користувача змінюється. Через 5 хвилин кількість легких іонів падає у 8 разів, а через 3 години є близькою до нуля. Це означає, що концентрація позитивних іонів зросла, а середні та важких негативно зраджених частинок знизилась. Така зміна балансу іонного складу повітря призводить до несприятливого впливу на здоров'я користувачів ВДТ [39, 42].

Відповідно до вимоги щодо рівня іонізації повітря на робочих місцях для користувачів ВДТ ПК оптимальною кількість іонів в 1 $см^3$ має бути: n+ = 1500-3000; n- = 3000-5000 [39]. Оптимальні та допустимі норми встановлені «Санитарно-гигиеническими нормами допустимых уровней ионизации воздуха производственных и общественных зданий» №2152-80, ДСан ПіН 3.3.2.007-98 та НПАОП 0.00-1.28-10.

Для забезпечення нормованого мікроклімату та рівня іонізації повітря на робочих місцях користувачів можна застосовувати системи загальнообмінної припливно-витяжної вентиляції, пристрої місцевої вентиляції, установки штучного зволоження, а також установки генерації негативних іонів (аероіонізатори) [42].

Відповідно до ГОСТ 12.2.032-78 конструкція робочого місця і взаємне розташування всіх його елементів повинні відповідати антропометричним, фізіологічним і психологічним вимогам, а також характеру роботи. Конструкцією робочого місця повинно бути забезпечено оптимальне положення працюючого, яке досягається регулюванням: висоти робочої поверхні, сидіння і простору для ніг, а також відповідати сучасним вимогам ергономіки [43].

ДСанПіН 3.3.2.007-98 встановлює необхідно основні вимоги до організації робіт, пов'язаних із використанням ВДТ і ЕОМ. При розміщенні робочих столів з ВДТ відстань між бічними поверхнями ВДТ має бути не меншою 1,2 м, а відстань між тильними поверхнями екранів ВДТ - не меншою 2,5 м. Висота робочої поверхні робочого столу з ВДТ має бути в межах 680 - 800 мм, а ширина і

глибина - забезпечувати можливість виконання операцій у зоні досяжності моторного поля (рекомендовані розміри: 600 - 1400 мм, глибина - 800 - 1000 мм). Робоче місце повинно бути забезпечено підйомно-поворотним робочим стільцем з регульованим за висотою і кутом нахилу сидінням і спинкою [39,43].

Відповідно до «Роз'яснення щодо набуття права на перерву у зв'язку з роботою за комп'ютером» необхідно передбачати для користувачів ЕОМ залежно від характеру праці такі внутрішньозмінні режими праці та відпочинку при 8-годинній денній робочій зміні: для розробників програм із застосуванням ЕОМ - регламентовані перерви у роботі тривалістю 15 хв. після кожної години роботи за ВДТ, для операторів комп'ютерного набору - 10 хв. після кожної години роботи за ВДТ, для операторів ЕОМ з іншим характером праці - 15 хв. через кожні дві години роботи з використанням ВДТ [43].

Для оптимізації та збереження здоров’я працівників необхідно дотримуватися всіх вимог безпеки та санітарно-гігієнічні вимоги до обладнання робочих місць користувачів ЕОМ.

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

Надзвичайна ситуація (НС) – порушення нормальних умов життя і діяльності людей на об’єкті або території, спричинене аварією, катастрофою, стихійним лихом, епідемією, епізоотією, епіфітотією, яка за своїми наслідками становить загрозу життю або здоров’ю населення чи призводить до завдання матеріальних збитків [44].

Розглянемо найбільш вірогідний варіант НС техногенного характеру для працівника з ЕОМ, а саме пожежу.

Пожежа – це неконтрольоване горіння, яке супроводжується знищенням матеріальних цінностей і створює небезпеку для життя людей. Пожежа, погашена у самій початковій стадії розвитку, називається загорянням [44].

Пожежна безпека — це комплекс організаційних заходів та технічних засобів, спрямованих на попередження та гасіння пожежі.

Правила пожежної безпеки – це комплекс положень, що визначають вимоги й встановлюють норми пожежної безпеки при будівництві та (або) експлуатації об'єкта. Нині є чинними «Правила пожежної безпеки в Україні», які обов'язкові для виконання всіма підприємствами галузі.

Увесь комплекс заходів та засобів з пожежної безпеки об’єкта прийнято поділяти на три групи – системи попередження пожежі, пожежного захисту та організаційно-технічних заходів.

Горіння виникає за таких трьох умов: наявності окисника, наявності горючої речовини, наявності температури, за якої горюча речовина може самостійно горіти. Якщо немає хоча б однієї із цих умов, горіння стає неможливим.

Серед найбільш поширених та небезпечних є джерела запалювання, які пов’язані з такими тепловими проявами електричної енергії, до них відносяться короткі замикання в електричних мережах, струмові перевантаження, розряди статичної та атмосферної електрики, електричні іскри, розігрів місць з'єднання проводів [45].

Заходи запобігання виникненню пожежі та вибуху, первинні засоби пожежогасіння. Ліквідувати вогнище можна, усунувши одну із трьох умов виникнення горіння. Припинити доступ кисню до горючої речовини або/і понизити її температуру можна, якщо своєчасно використати первинні засоби гасіння пожеж.

Для ліквідації пожежі у початковій стадії її розвитку силами персоналу об’єктів застосовуються первинні засоби пожежогасіння. До них відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, ящики з піском, пожежні відра, совкові лопати, ломи, сокири тощо), системи автоматичного пожежогасіння [45].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступеня вогнестійкості. Стіни кабін виготовляються з негорючих матеріалів. Дозволяється виготовляти їх зі скла та металевих конструкцій [42,45].

У приміщеннях, де безпосередньо встановлено ЕОМ забороняється:

- залишати без нагляду електричну апаратуру, що використовується;
- зберігати постійно в залах ЕОМ носії інформації, запасні блоки та деталі в кількості більшій, ніж необхідно для поточного використання;
- користуватися груповими розетками на горючій панелі;
- використовувати килими та доріжки із синтетичних матеріалів;
- ставити на вікна глухі грати;
- застосовувати електронагрівальні побутові прилади;
- курити та застосовувати відкритий вогонь .

Для захисту від пожежі приміщення з наявністю ЕОМ треба використовувати вуглекислотні вогнегасники або аерозольні водопінні вогнегасники. Приміщення, у яких розміщені ЕОМ, треба оснащувати переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 м^2 площі приміщення. Підходи до засобів пожежогасіння повинні бути вільними.

Усі працівники при прийнятті на роботу у і в процесі праці повинні проходити протипожежний інструктаж, перевірку знань з питань пожежної безпеки [42]. Щоб при виявленні пожежі (ознак горіння) кожен знав порядок дії:

- негайно сповістити про це по телефону в пожежну охорону;
- повідомити про пожежу керівника чи відповідну компетентну посадову особу та (або) чергового по об'єкту;
- прийняти (за можливості) заходи щодо евакуації людей, гасіння (локалізації) пожежі і схоронності матеріальних цінностей;
- надати медичну допомогу, якщо є необхідність.

Засоби протипожежного захисту слід утримувати у справному стані. Приміщення з ЕОМ, повинні бути оснащені системою автоматичної пожежної сигналізації та автоматичними установками пожежогасіння [40]. Усі працівники повинні вміти користуватись наявними вогнегасниками, іншими первинними засобами пожежогасіння, знати місце їх знаходження.

Отже, для забезпечення оптимальний умов праці на комп'ютеризованому робочому місці необхідно визначити важкість праці відповідно до категорії, на підставі чого проводиться аналіз існуючих умов і їх нормування відповідно до існуючих стандартів. До параметрів умов праці на робочому місці користувача ЕОМ відносяться: освітленості, мікроклімат, рівень шуму та вібрацій, іонний склад повітря, ергономічні характеристики робочого місця, а також режим праці і відпочинку. Нормування цих параметрів необхідне для того, щоб запобігти впливу шкідливих виробничих факторів , травматизму і забезпечити комфортні та безпечні умови праці для здоров'я людини.

До небезпечних факторів на комп’ютеризованому робочому місці також відноситься ризик виникнення пожежі. Але при дотриманні всіх вимог до побудови та експлуатації приміщень, які призначені для роботи на ЕОМ, правил безпеки, а також проведення систематичного інструктажу для персоналу, можна забезпечити належний рівень пожежної безпеки та зменшити вірогідність виникнення пожежі.

4.3 Вибір первинних засобів пожежогасіння

Первинні засоби пожежогасіння слугують для гасіння пожеж в початковій стадії їх розвитку до прибуття пожежних підрозділів. До первинних засобів пожежогасіння відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, грубововняної тканини або повсті, ящики з піском, бочки з водою, пожежні відра, совкові лопати) та пожежний інструмент (гаки, ломи, сокири тощо) [44].

Первинні засоби пожежогасіння розміщують на спеціальних щитах. Щити встановлюють з таким розрахунком – один щит на 5000 м^2. Місця розміщення первинних засобів пожежогасіння зазначаються у планах евакуації [45,46].

Критеріями вибору типу і необхідної кількості вогнегасників для захисту об'єкта є [47]:

- рівень пожежної небезпеки об'єкта (будинку, споруди, приміщення);

- клас пожежі горючих речовин та матеріалів, наявних у ньому;
- придатність вогнегасника для гасіння пожежі певного класу та відповідність умовам його експлуатації;
- вогнегасна здатність вогнегасника конкретного типу;
- категорія приміщення за вибухопожежною або пожежною небезпекою;
- наявність у приміщенні модульної установки автоматичного пожежегасіння;
- площа об'єкта.

Приміщення з ЕОМ відповідно до стандарту ISO 3941-77 за класом пожежі горючих речовин та матеріалів відповідають класу Е – пожежі, пов‘язані з горінням електроустановок.

Для всіх споруд і приміщень, в яких експлуатуються відеотермінали та ЕОМ, повинна бути визначена категорія з вибухопожежної і пожежної безпеки відповідно до НАПБ Б.03.002-2007 “Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою”, та клас зони згідно з ПУЕ. Відповідні позначення повинні бути нанесені на вхідні двері приміщення [46].

Виділяють наступні категорії приміщень за вибуховопожежої та пожежної безпеки: А, Б, В, Г, Д. Приміщення з ПЕОМ можна віднести до категорії В.

Відстань від можливого осередку пожежі до місця розташування вогнегасника не повинна перевищувати: 20 м для громадських будівель та споруд; 30 м – для приміщень категорій А, Б, В (горючі гази та рідини); 40 м- для приміщень категорій В, Г; 70 м – для приміщень категорії Д.

Приміщення, обладнані модульними установками автоматичного пожежогасіння, якщо в них немає постійного перебування людей, можуть забезпечуватися вогнегасниками на 50 % від їх норм належності для цих приміщень [47].

Вибір типу та необхідної кількості вогнегасників проводиться згідно з нормами належності для переносних та пересувних вогнегасників.

При захисті від пожежі приміщення з наявністю ПЕОМ, телефонних станцій тощо слід використовувати вуглекислотні вогнегасники або аерозольні водопінні

вогнегасники. Такі приміщення слід оснащувати переносними вуглекислотними вогнегасниками з розрахунку один вогнегасник ВВК-1,4 (старе позначення - ОУ-2) чи ВВК-2 (старе позначення - ОУ-3) або один ВВПА-400 (вогнегасник водопінний аерозольний з масою заряду вогнегасної речовини 400 г) на три ПЕОМ, але не менше ніж один вогнегасник зазначених типів на приміщення [47].

Для приміщення у якому розташоване робоче місце з ПЕОМ має категорію В за вибухопожежною та пожежною безпекою площею 58м^2 (клас пожежі горючих речовин та матеріалів – Е) має захищатися 2 переносними вуглекислотними вогнегасниками місткістю 5л або 2 порошковими з величиною заряду 5кг. А також 1 пересувним вуглекислотним вогнегасниками місткістю 80л. Відстань між вогнегасниками та місцем можливого загорання не повинна перевищувати 40 м.

ВИСНОВКИ

У кваліфікаційній роботі вирішена важлива науково-практична задача підвищення ефективності прихованого (стеганографічного) каналу зв’язку шляхом розробки стеганографічного методу, стійкого до атак проти вбудованого повідомлення, у тому числі до атаки стиском та накладанню шумів, на основі досліджень, у результаті яких було обрано у якості області для вбудовування додаткової інформації область сингулярного розкладання блоків матриці ЦЗ-контейнера, отриманих шляхом стандартної розбивки матриці.

Алгоритмічна реалізація розробленого методу є стійкою до атаки стиском з втратами, маючи при найбільш часто використовуваному коефіцієнті якості $QF = 75$ 2,93% помилок при декодуванні ДІ, а і в умовах накладання шумів: гауссівського та мультиплікативного, з параметром $D = \{0.001, 0.0001\}$, що забезпечує надійність сприйняття формованого стеганоповідомлення, кількість помилок при декодуванні додаткової інформації не перевищує 1,56%.

Ефективність розробленого алгоритму порівняна з аналогами в умовах найчастіше використовуваної атаки проти вбудованого повідомлення - атаки стиском. У порівнянні з 2-ма найкращими аналогами, використаними для порівняння, розроблений алгоритм при $QF = 60$ підвищує ефективність на 23%, а при $QF=90$ на 1%. При цьому алгоритми, з якими проводилося порівняння, позиціонуються як стійкі до атаки стиском, а розроблений алгоритм, який опирається на новий математичний базис, є взагалі стійким до атак проти вбудованого повідомлення, що дозволяє говорити про досягнення мети роботи та підвищення ефективності прихованого (стеганографічного) каналу зв’язку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Информационное противоборство в современных условиях. Л.Г. Пирцхалава и др. К.: ЦП «Компринт», 2019. 226 с.,
2. Козюра В.Д. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 144 с.
3. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України. 2014. 5. С. 65–69.
4. Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации. М.: АСТ: Астрель, 2011. – 656 с.
5. Мельник С.В., Кащук В.І. Методи цифрової стеганографії: стан та напрями розвитку *Інформаційна безпека людини, суспільства, держави*. 2013. № 3 (13). С.65-70.
6. Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. Сучасні стеганографічні методи захисту інформації. *Науково-технічний журнал «захист інформації»*. 2011. №1. С.1-7.
7. Навроцький Д.О. Методи комп'ютерної стеганографії. *Вісник Національного технічного університету України "КПІ". Серія – Радіотехніка. Радіоапаратобудування.* 2007. №3. С.105-108.
8. Абазина, Е.С., Ерунов А.А. Цифровая стеганография: состояние и перспективы. *Системы управления, связи и безопасности*. 2016. №2. С. 181-201.
9. Li B. A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing. 2011. 2(2). P. 142–172
10. Грибунин, В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М. :СОЛОН-Пресс, 2009. 272 с
11. Pfitzmann B. Information Hiding Terminology, in Information Hiding, *Springer Lecture Notes in Computer Science,* v.1174. 1996. P.347-350.

12. Генне О.В. Основные положения стеганографии. *Журнал "Защита информации. Конфидент"*. 2000. №3.
13. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії : Навч. посіб. для студентів і аспірантів. — Вінниця: ВДТУ, 2003.
14. Saleh M.E., Aly A.A., Omara F.A. Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications.* 2016. 7(6). P. 390–397.
15. Кобозева А. А., Мельник М. А. Формальные условия обеспечения устойчивости стеганометода к сжатию. *Сучасна спеціальна техніка.* - 2012. № 4. С. 60-69.
16. J. Tao et al Towards robust image steganography. *IEEE Transactions on Circuits and Systems for Video Technology.* 2019. 29(2). P. 594–600.
17. Конахович, Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев : МК-Пресс, 2006. — 288 с.
18. Fan, C.-H., Huang H.-Y., Hsu W.-H A robust watermarking technique resistant Jpeg compression. *Journal of Information Science and Engineering.* 2011. Vol. 27, Iss. 1. — P. 163–180.
19. Кобозева А.А., Лебедева Е.Ю., Костырка О.В. Стеганопреобразование пространственной области изображения-контейнера, устойчивоек атакам против встроенного сообщения. *ProblemeleEnergeticiiRegionale*. 2014. 1(24). URL: http://journal.ie.asm.md/ru/contents/elektronnyij-zhurnal-n-124-2014
20. Костирка О.В. Модифікація стійкого до збурних дій стеганоперетворення просторової області зображення-контейнера. *Інформатика та математичні методи в моделюванні.* 2016. 6(1). С. 85–93.
21. Nasir I.A., Abdurrman A. A robust color image watermarking scheme based on image normalization. *Proceedings of the World Congress on Engineering (WCE 2013)*. London, 2013. Vol. III.
22. Patra J.C., Kishore A.K.,Bornand C. Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital

media authentication. *Proceedings of 2011 IEEE International Conference on Systems, Man, and Cybernetics.* Anchorage, 2011. P. 2940-2945.

23. Li, B. A Survey on Image Steganography and Steganalysis. *Journal of Information Hiding and Multimedia Signal Processing.* 2011. Vol.2, No.2. PP.142–172.
24. Rawat, H., Kumar A., Kumar S. Robust Digital Image Watermarking Scheme for Copyright Protection. *International Journal of Computer Applications*. 2013. Vol.75, No.18. P.27-32.
25. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации. *Искусственный интеллект.* — 2007. — № 4. — С. 531–538.
26. Кобозева, А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009.
27. Кобозева АА., Мельник М.С. Анализ чувствительности сингулярных векторов матрицы изображения-контейнера как основа стеганоалгоритма, устойчивого к сжатию с потерями. *Захист інформації*. 2013. Том 15, №2.
28. Кобозєва А.А., Хорошко В.О. Аналіз захищеності інформаційних систем. Київ: ДУІКТ, 2010.
29. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с
30. Шелест М.Э., Варда Т.В., Родюк І.І. Стеганографічний метод стійкий до збурних дії. *Інформатика та математичні методи моделювання*. 2019. Vol.9. №4.
31. Кобозева А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений. *Праці Одеського політехнічного університету*. 2014. Вип. 2(44). С.136-146.
32. Wang, S.H., Lin Y.P. Wavelet tree quantization for copyright protection watermarking. *EEE Transactions on Image Processing*. 2004. Vol. 13, Iss. 2. PP. 154–165.

33. Li, E., Liang H. , Niu X. An integer wavelet based multiple logo-watermarking scheme. *Proceedings of the IEEE WCICA*. 2006. PP.10256–10260.

34. Колесников, М.В. Метод скрытой передачи данных в оптическом канале видеокамеры. *Инженерный вестник*. — М. : ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», 2013. № 2. URL: http://engbul.bmstu.ru/doc/543251.html

35. Колесников, М.В. Метод скрытой передачи данных в оптическом канале видеокамеры. *Инженерный вестник.* — М. : ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», 2013. № 2. URL: http://engbul.bmstu.ru/doc/543251.html

36. Бобок И.И., Кобозева А.А., Батиене Л.Е. Усовершенствование стеганографического алгоритма, основанного на sign-нечувствительности сингулярных векторов блоков матрицы изображения. *Інформатика та математичні методи в моделюванні*. 2017. 7(1-2). С. 19–28

37. Мельник, М.А. Повышение скрытой пропускной способности стеганографических алгоритмов, устойчивых к атаке сжатием. *Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка.*. 2013. Вип. 41. С. 56–62

38. Lin, W.-H., Wang Y.-R., Horngetal S.-J. A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications*. 2009. No.36. P.11509–11516

39. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин: N 7 від 10.12.98. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text

40. Голінько, В.І., Чеберячко С.І., Шибка М.В., Яворська О.О. Моніторинг умов праці: підручник. М-во освіти і науки України; Нац. гірн. ун-т. – 2-ге вид. – Д.: НГУ, 2014. – 230 с.

41. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин. НПАОП 0.00-1.31-99. URL: https://zakon.rada.gov.ua/laws/show/z0382-99 (дата звернення: 10.06.2019)

42. Жидецький, В. Ц. Охорона праці користувачів комп'ютерів. – Львов, Афіша 2000. – С.74 – 75

43. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования. URL: http://docs.cntd.ru/document/1200003913.
44. Кодекс цивільного захисту України, 2013, № 34-35, ст.458 https://zakon.rada.gov.ua/laws/show/5403-17#Text
45. Наказ про затвердження Правил пожежної безпеки в Україні від 19.10.2004 №126. Дата звернення - 24.11.2020
46. Атаманчук П. С., Мендерецький В. В., Панчук О. П. Чорна О. Г. Безпека життєдіяльності. Навч. посіб. - К.: Центр учбової літератури, 2011. - 276 с.
47. Охорона праці та промислова безпека: навч. посіб. для студ. вищ. навч. закл. / Ткачук, К.Н. за ред. д. т. н., проф. К. Н. Ткачука і к. т. н., доц. В. В. Зацарного. - К. : Лібра, 2010. - 559 с.