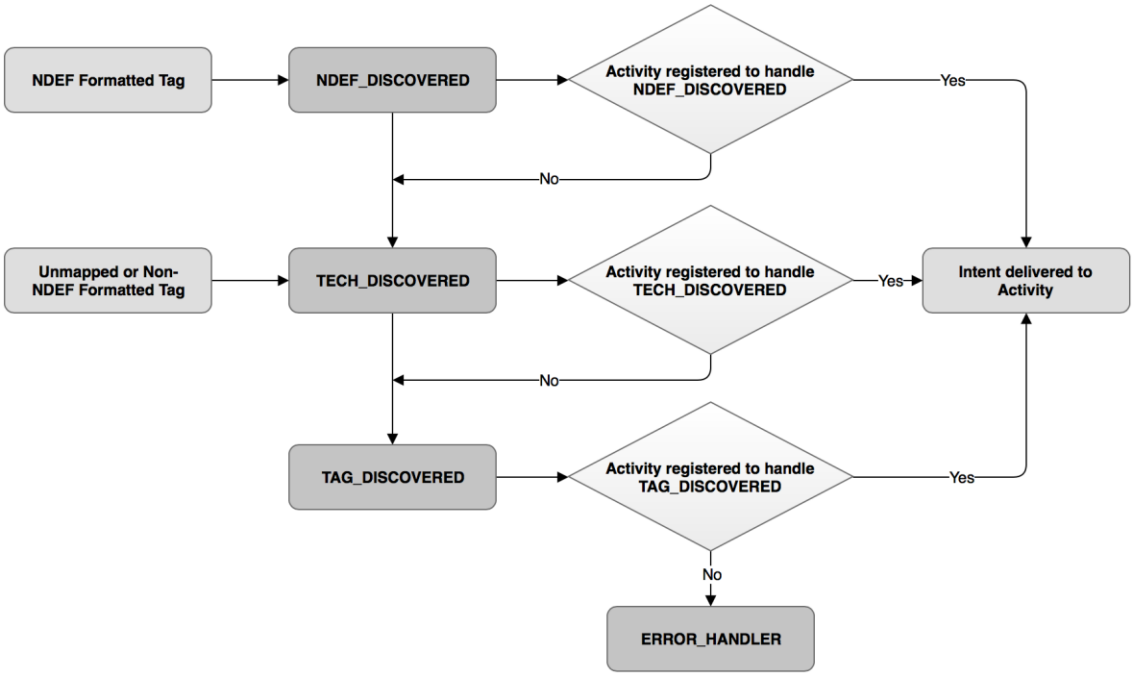

Рисунок 1 - Діаграма активності при виявленні NFC-мітки

Висновок

В процесі виконання роботи було отримано наступні результати:

- розроблено програмний модуль для ідентифікації сигналів, який дозволяє працювати з різними об’єктами, які є носіями NFC-міток;
- розроблено мобільний додаток для ідентифікації об’єктів з використанням технології NFC.

Список використаних джерел

1. І. М. Голдовський. Банківські мікропроцесорні карти - ЦІПСіР: Альпіна Паб, 2010. - 686 с. [Електронний ресурс]. – Режим доступу: https://goo.gl/YDcSq5
2. Android.nfc Офіційна документація Google. [Електронний ресурс]. Режим доступу: https://goo.gl/0EqCQQ
3. Ліанг Цанг. Зона розробки компанії Intel. Розробка NFC додатків на Android. [Електронний ресурс]. – Режим доступу: https://goo.gl/6gyOxI

УДК 004. 4

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИСТУ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ ПРИМІТИВІВ

Звольський О.А., Заріцький Б.Б.
Тернопільський національний економічний університет, магістранти

I. Постановка проблеми

На даний час доцільною є розробка стеганографічних систем, які можуть підвищити ефективність вирішення проблем захисту інформації. Перевага стеганографічного захисту полягає в тому, що він дає можливість приховано передавати закриту інформацію одночасно з відкритою (видимою) інформацією, яка не має конфіденційного характеру. При цьому з'являється можливість уникнути прямих атак на закриту інформацію [1].

Тому розробка програмного забезпечення, що дозволяє передавати великий об’єм інформації в зображеннях таким чином, щоб зловмисник не зміг виявити факт її наявності є актуальним.

II. Мета роботи

Метою даної праці є створення програмного забезпечення для системи захисту

стеганографічних примітивів.

III. Програмне забезпечення для системи захисту стенографічних примітивів

На основі аналізу алгоритмів та методів побудови системи захисту розроблено алгоритм програми, призначеної для захисту інформації на основі стеганографічних примітивів [2]. Спрощений алгоритм програми зображено на рисунку 1.

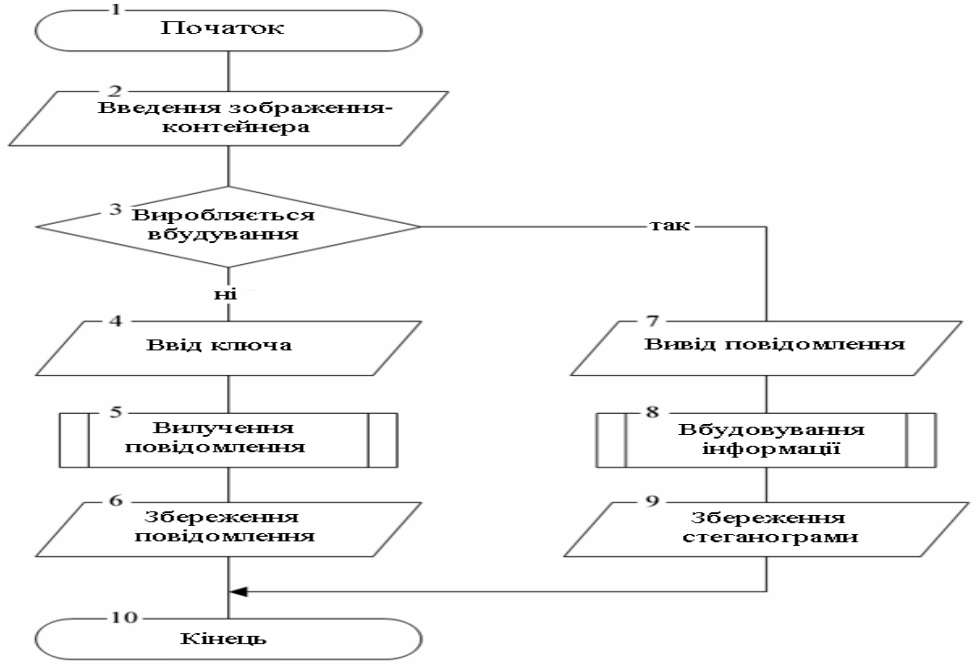

Рисунок 1 - Блок-схема алгоритму програми

Користувачеві надається можливість виконувати основні дії, передбачені в програмі, а саме:

- вбудовувати інформації в зображення;
- вилучати вбудовану в зображення інформацію;
- проводити захист інформації за допомогою ключа;
- слідкувати за показником процесу вбудовування;
- надано можливість побачити кількість вбудованих байтів в області зображення;

Вхідними даними для розробленого програмного забезпечення будуть текстові файли з конфігураційними даними, а вихідними даними можна вважати інформацію, яку вилучили із зображення.

Головне вікно програми зображено на рисунку 2.

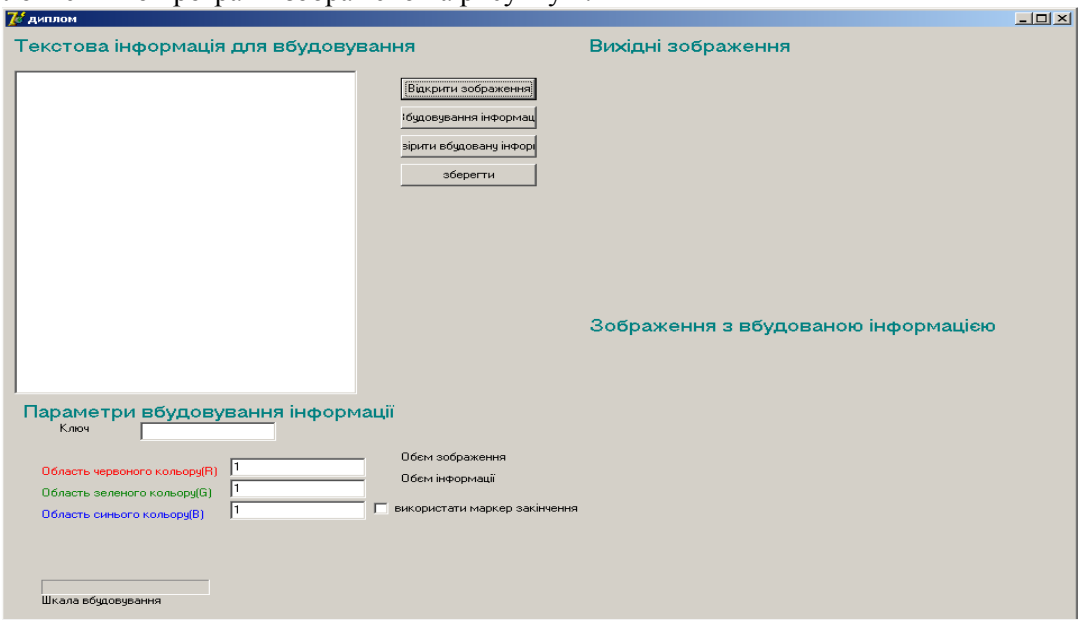

Рисунок 2 - Головне вікно програми на початку роботи

Висновок

Розроблено програмне забезпечення для системи захисту інформації на основі стеганографічних примітивів, яке надає можливість приховано передавати одночасно закриту і відкриту інформації.

Список використаних джерел

1. Барсуков В.С., Романцов А.П. Комп'ютерна стеганографія: вчора, сьогодні, завтра. Технології інформаційної безпеки XXI століття. Матеріали Internet-ресурсу «Спеціальна техніка» (http://st.ess.ru/).
2. Бобровский С. Delphi 6 и Kylix: Библиотека программиста. – СПб.: Питер, 2002. – 560 с.

УДК 004.056

МОДИФІКОВАНИЙ МЕТОД ВИЯВЛЕННЯ РОЗМИТТЯ ЦИФРОВОГО ЗОБРАЖЕННЯ

Зоріло В.В. [1)], Головко Ю.О.[2)], Якименко І.З.[3)], Гураль І.В.[4)]

[1)] *Одеський національний політехнічний університет, к.т.н*

Тернопільський національний економічний університет

[2)] *магістрант;* [3)] *к.т.н;* [4)] *викладач*

І. Постановка проблеми

Існуючі методи виявлення фальсифікацій цифрового зображення[1-3], як правило, недієздатні при малому розмірі фальсифікованої області (зокрема, коли ця область має розміри блоку, отриманого при стандартному розбитті матриці зображення) [4], хоча саме такі області дуже часто використовуються в процесі фальсифікацій; вони, як правило, не враховують результатів постобробки фальсифікованого цифрового зображення графічними редакторами, яка є практично обов'язковою складовою несанкціонованих змін зображень.

Як показує практика та факти, відомі з відкритих джерел, одним з програмних інструментів, що найчастіше використовується під час обробки цифрового зображення є розмиття (хоча розмиття часто використовується в фотоіндустрії для зовсім «некримінальних» цілей: надання певного ефекту як зображенню в цілому, так і його частині, наприклад, для акцентування уваги на деякому об'єкті (об'єкт – чіткий, в фокусі, а остання область розмита); усунення дефектів зображення, що виникають, наприклад, при скануванні, при компресії; для усунення на зображенні природних дефектів шкіри як звичайних (шрами і тощо), так і вікових (зморшки)).

У зв'язку з цим можна констатувати, що задача детектування порушення цілісності цифрового зображення не є до кінця вирішеною, вона залишається важливою та потребує застосування нових для цієї галузі досліджень математичних інструментів, розробки нових алгоритмів виявлення порушення цілісності цифрових сигналів.

ІІ. Мета роботи

Основною метою даної роботи є підвищення ефективності виявлення розмиття цифрового зображення шляхом модифікації методу, заснованого на аналізі сингулярних чисел.

ІІІ. Модифікований метод виявлення розмиття цифрового зображення

В основі виконаної у роботі модифікації лежить метод виявлення розмиття цифрового зображення, заснований на аналізі сингулярних чисел. Візуальним результатом розмиття є згладжування контурів, що призведе до зменшення високочастотної складової сигналу. Основні положення даного методу полягають у наступному. Матрицю цифрового зображення розбивають стандартним чином на блоки 8×8. Для кожного блоку знаходять множину СНЧ. Для п'ятьох найменших сингулярних чисел у кожному блоці будують лінійну апроксимацію, і для апроксимуючої функції визначають похідну, значення якої (константа) являє собою коефіцієнт швидкості росту зазначених сингулярних чисел. Якщо максимальне значення коефіцієнту швидкості росту серед усіх 8×8-блоків не перевищує порогового значення, зображення вважають розмитим. Якщо середнє значення коефіцієнту швидкості росту серед усіх 8×8-блоків перевищує порогове значення – зображення вважають нерозмитим. В інших випадках метод передбачає додаткову перевірку. Додаткова перевірка полягає в проведенні експертом навмисного розмиття цифрового зображення з