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

подальшим порівнянням аналізованих параметрів. Якщо експертне розмиття для зображення є першим, аналізовані параметри зменшуються більш ніж у 2 рази. При повторному розмитті відбувається зменшення шуканих параметрів в два і менше разів. Ця особливість дозволяє зробити висновок про те, чи є проведене експертом розмиття повторним для зображення, або ж його застосовано вперше.

При здійсненні фотомонтажу практично завжди виникає необхідність у використанні такого інструменту, як розмиття зображення. Особливо актуальним стає розмиття, коли необхідно обробити контури, зробити фальсифікацію непомітною при візуальному аналізі ЦЗ. Як показує практика, доцільно розмивати не тільки контур заміщаючої області, а й все зображення. Розмиття при цьому має бути настільки великим, щоб приховати фальсифікацію, і настільки маленьким, щоб якість (чіткість) ЦЗ не викликало сумнівів в його автентичності.

Другою причиною розмиття зображення в цілому може бути мета «обійти» вже існуючі методи виявлення фотомонтажу, описаного вище. Сліди навмисного розмиття зображення або його частини свідчать про порушення його автентичності та можуть вказувати на наявність фальсифікації. Отже, виявлення слідів розмиття дає підставу не використовувати ЦЗ в якості достовірного документа.

Третьою причиною розмиття зображення, як уже згадувалося, може бути стеганографічна атака цифрового зображення як стегоконтейнера (контейнер – так називається будь-яка інформація, яка використовується для приховування таємного повідомлення. Стегоконтейнер – контейнер, що містить таємне послання) [5].

Розмиття часто використовується в фотоіндустрії з некримінальною метою. Це може бути надання бажаного ефекту як зображенню в цілому, так і його частини, наприклад, для акцентування уваги на деякий об'єкт за допомогою зменшення глибини різкості зображуваного простору (наприклад, макрозйомка – об'єкт чіткий, у фокусі, решта частини зображення розмита, не в фокусі). Також розмиття використовують з метою усунення дефектів ЦЗ, які можуть виникнути при скануванні або при стисненні і т.п. Графічні редактори реалізують безліч видів розмиття, наприклад, в графічному редакторі Adobe Photoshop реалізовано 11 видів. У рамках специфіки розглянутої галузі використання фотомонтажу найчастіше використовують розмиття за Гаусом, основною характеристикою якого є радіус розмиття, однак при постобробці фальсифікованого ЦЗ взагалі можуть бути використані різні види розмиття з довільними параметрами.

IV. Висновки

В роботі вдосконалено метод виявлення розмиття цифрових зображень, який заснований на загальному підході до аналізу стану та технології функціонування інформаційних систем, що призвело до підвищення ефективності виявлення результатів розмиття цифрових зображень засобами графічних редакторів. Доведено отримані наукові результати до конкретного алгоритму, що може бути використаний як складова систем захисту інформації, інформаційних систем різного наповнення будь-якого закладу, підприємства, тощо.

Список використаних джерел

1. Кобозєва А.А. Метод виявлення фальсифікації цифрового зображення в умовах збурних дій /А.А. Кобозєва, В.В. Зоріло// Збірник наукових праць військового інституту національного університету імені Тараса Шевченка. – 2009. – № 20. – С.147-153.
2. Кобозева А. А.Анализ информационной безопасности: монография / А.А.Кобозева , В. А. Хорошко. - К. : ГУИКТ, 2009. - 251 с. - Библиогр.: с. 240-247.
3. Зорило В.В. Выявление результатов обработки цифрового изображения некоторыми программными средствами /В.В. Зорило, А.А. Кобозева //Вісник Східноукраїнського національного університету ім. Володимира Даля. – 2010. – № 9(151),Ч.1. – С.92-97.
4. Гантмахер Ф.Р. Теория матриц / Ф.Р.Гантмахер. — М.: Наука, 1988. — 552 с.
5. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф.Конахович, А.Ю.Пузыренко. — К.: МК — Пресс, 2006. — 288 с.