ПБС, абсолютне значення такого параметру для всіх підблоків може відрізнятися від сигналу до сигналу.

Був проведений обчислювальний експеримент. Визначалось максимальне значення En для оригінальних та фальсифікованих аудіо. Аудіо сигнали були фальсифіковані за допомогою аудіо редактору Free Audio Editor, шляхом заміни частини одного аудіо на частину іншого аудіо сигналу.

Обчислювальний експеримент було проведено на 200 аудіо, серед яких були і оригінальні, і фальсифіковані аудіо сигнали, в якості порогового значення для відділення частини цифрового аудіо що містить фальсифікацію від оригінальних частин, було запропоновано використовувати значення 40.

Висновок

Розроблений програмний продукт надає можливість ефективного виявлення фальсифікації цифрового аудіо сигналу, має дружній інтерфейс, а результати аналізу є наглядними. Проведені експериментальні дослідження на реальних аудіо записах підтверджують ефективність та доцільність його використання.

Список використаних джерел

1. Гонсалес Р. Цифровая люработка зображений / Гонсалес Р. , Вудс Р. .-Техносфера,2005 ,1011 с.
2. Ленков С.В. Методы и средства защиты информации в 2-х т. / Ленков С.В., Пергудов Д.Л.: К,,2008,,.654 с.
3. Хорошко Л. Методы и средства защиты информации / Хорошко Л, Чекачков А. –К.:Юниор,-2003.-501 с.

УДК 004.42

МЕТОД СТІЙКОГО ЦИФРОВОГО ВОДЯНОГО ЗНАКУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ КОНТЕНТУ МОБІЛЬНОГО ПРИСТРОЮ

Гончар Л.І.[1)], Тіхорський О.М.[2)]

Тернопільський національний економічний університет

[1)] к.е.н., доцент; [2)] магістрант

І. Постановка проблеми

На сьогоднішній день для перевірки цілісності та аутентифікації електронної інформації, що знаходиться у вільному доступі, широке використання отримали методи цифрового водяного знаку (ЦВЗ). Вони реалізовані програмно та/або апаратно для більшості інформаційних мереж підприємств, банків, державних структур, є програмні реалізації для домашнього використання на персональних комп'ютерах (ПК), випускаються фотокамери з вбудованими засобами ЦВЗ тощо. Широкий попит та використання мобільних пристроїв для створення та передачі електронної інформації обумовлює актуальність задачі програмної реалізації методу ЦВЗ для підвищення ефективності контенту мобільних пристроїв [2,3].

Із проведеного аналізу існуючих методів реалізації ЦВЗ можна зробити наступні висновки:

а) для аутентифікації контенту мобільного пристрою на платформі Windows Phone необхідно обрати робастний метод ЦВЗ;

б) стійкість стеганографічних методів не залежить від області вбудовування додаткової інформації, тож переважаючими є методи просторової області вбудовування;

в) для досягнення мети роботи найбільш придатним є метод Куттера–Джордана–Боссена як метод нанесення стійкого ЦВЗ, що працює в просторовій області цифрового зображення та найкраще задовільняє потребам захисту фотографій на мобільному пристрої .

ІІ. Мета роботи

Метою даної наукової роботи є програмна реалізація методу стійкого ЦВЗ на платформі Windows Phone для підвищення ефективності захисту контенту мобільного пристрою.

ІІІ. Використання методу Куттера–Джордана–Боссена для вбудовування ЦВЗ

Окрім робастності, алгоритм Куттера–Джордана–Боссена досить простий у реалізації: для вбудовування ЦВЗ немає необхідності виконувати громіздкі лінійні перетворення цифрового зображення (ЦЗ), ЦВЗ вбудовується за рахунок маніпуляції колірних складових.

Кожне зображення складаються з пікселів, які представляють собою об'єднання трьох колірних матриць: червоної – R, зеленої – G, синьої – B, та матриці прозорості –A. Вбудовування

виконується в канал синього кольору, так як до синього кольору система людського зору найменш чутлива [9]. Нехай біт який вбудовуємо, контейнер I={R,G,B}, p=(x,y) псевдовипадкова позиція, в якій виконується вкладення. Секретний біт вбудовується в канал синього кольору шляхом модифікації яскравості:

$$l(p) = 0{,}299r(p) + 0{,}587g(p) + 0{,}114b(p), \quad (1)$$

$$b'(p) = \begin{cases} b(p) + ql(p), & \text{якщо } s_i = 0, \\ b(p) - ql(p), & \text{якщо } s_i = 1 \end{cases} \quad (2)$$

де q - коефіцієнт, що задає енергію біта даних, що вбудовується (задається виходячи з функціонального призначення і особливості стеганосистеми). Його значення залежить від призначення схеми. Чим більше q, тим вище робастність вкладення, але тим сильнішає його помітність.

Для реалізації програмного продукту була вирішена задача визначення позиції пікселів цифрового зображення, в які виконувалося вбудовування ЦВЗ.. Замість використання псевдовипадкової послідовності пікселів для вбудовування бітів цифрового водяного знаку запропоновано використовувати послідовність пікселів, що рівномірно розподілені по всьому зображенню. Рівномірне нанесення ЦВЗ та його десятикратне повторення дозволяють підвищити ефективність захисту цифрового зображення та ефективність вилучення вбудованої інформації не зважаючи на несиметричність процедур вбудовування.

Реалізовано перевірку зображення на наявність ЦВЗ та функціональну можливість викладати зображення з вбудованим ЦВЗ в Інтернет.

Висновок

Таким чином, в роботі програмно реалізований метод Куттера–Джордана–Боссена для Windows Phone, використання якого для вбудовування стійкого ЦВЗ знаку у зображення, створені та збережені на мобільному телефоні, значно підвищить ефективність захисту контенту мобільного пристрою.

Список використаних джерел

1. Грибунин, В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев; – М : СОЛОН-Пресс, 2002. – 261 с.
2. Конахович, Г. Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю Пузыренко – К.: МК-Пресс, 2006. – 249 с.
3. Кустов, В. Н. Методы встраивания скрытых сообщений / В. Н. Кустов, А. А. Федчук // Защита информации. Конфидент.- 2000.- №3. – С. 34-37.

УДК 681.3

УДОСКОНАЛЕННЯ АЛГОРИТМУ ЗАГАЛЬНОГО РЕШЕТА ЧИСЛОВОГО ПОЛЯ НА ОСНОВІ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ

Кінах Я.І.[1)], Якименко І.З.[2)], Лаврик О.П.[3)]

[1)] *Тернопільський національний технічний університет імені Івана Пулюя, к.т.н., доцент;*
[2)] *Тернопільський національний економічний університет, к.т.н., доцент*
[3)] *Тернопільський національний економічний університет, магістрант*

І. Постановка задачі

Розробка й впровадження розподілених технологій у практику є актуальною задачею для підвищення рівня захисту інформації [1], раціонального використання інфраструктури установ різного відомчого підпорядкування, взаємодії з службами інших країн, розвитку виробництва засобів захисту інформації.

Головними вимогами до подібних систем є стабільність роботи, швидке відновлення в результаті збоїв програмного та апаратного забезпечення, робота в умовах повільних каналів зв'язку. Ці вимоги особливо ускладнюються у випадку необхідності проведення криптоаналізу в режимі реального часу та при застосуванні паралельних алгоритмів.