УДК 004.42

МЕТОД ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО АУДІО СИГНАЛУ ЗБЕРЕЖЕНОГО У ФОРМАТІ ІЗ ВТРАТОЮ ІНФОРМАЦІЇ

Гончар Л.І.[1)], Гасюк Н.І.[2)]
Тернопільський національний економічний університет
[1)] к.е.н., доцент; [2)] магістрант

І. Постановка проблеми

В сучасних умовах створення, зберігання та передачі інформації в електронному вигляді виникає можливість несанкціонованого доступу або модифікації цифрових сигналів, у тому числі цифрових аудіо (ЦА). Це обумовлено бурхливим розвитком програмних засобів для редагування цифрових сигналів, які дають можливість змінювати цифрові аудіо, тим самим не лише порушуючи цілісність, але і фальсифікуючи його.

Відомо, що переважними для використання є програмні методи пасивного захисту, які не потребують додаткової інформації для проведення перевірки цілісності сигналу. До області застосування цих методів відносяться аудіо сигнали, що збережені у форматі без втрат інформації.

У зв'язку з цим задача виявлення фальсифікації цифрового аудіо, збереженого у форматі із втратою інформації, є актуальною, але невирішеною в повному обсязі, проблемою.

ІІ. Мета роботи

Метою даної роботи є автоматизація процесу виявлення та локалізації фальсифікації цифрового аудіо, збереженого у форматі із втратою інформації.

ІІІ. Метод виявлення та локалізації фальсифікації цифрових сигналів

Серед програмних методів пасивного захисту інформації завдяки своїй простоті особливу увагу привертає метод виявлення і локалізації фальсифікації цифрового зображення (ЦЗ), збереженого у форматі із втратою інформації, заснований на дослідженні функції квадрату середньоквадратичного відхилення значень коефіцієнтів дискретного косинусного перетворення (ДКП) від значень повторно відквантованних коефіцієнтів ДКП матриці ЦЗ з різними кроками квантування [2].

Для виявлення фальсифікації пропонувалося аналізувати функцію:

$$F(q) = \sum_{i=1}^{n} (f_i - f_i^q)^2 \quad , \tag{1}$$

де n – кількість коефіцієнтів ДКП, які відповідають заданій частоті; $\underline{f_i}$– коефіцієнт ДКП; f_i^q– визначається за формулою (2):

$$f^{\cdot} = \left[\frac{f_{\cdot}}{q} \right] q \quad , \; q \in (1,30] \tag{2}$$

Загалом до переваг зазначеного методу можна віднести наступне:

- для аналізу цифрового зображення не потрібна додаткова інформація про технічні або програмні характеристики фотоапарату, на якому цифрове зображення було створено;
- виявлення фальсифікації у деякому підблоці сигналу (ПБС) одночасно дає відповідь і про її локалізацію у зображенні;
- метод ефективно працює при наявності шумів округлення значень яскравості пікселів матриці цифрового зображення, тому може бути ефективно використаний на практиці;
- при дотриманні умов щодо розбиття цифрового зображення на підблоки сигналу при використанні розробленого методу може бути виявлена фальсифікація як великих (до 50% розміру самого зображення), так і малих розмірів (порядку 20х20 пікселів).

У розглянутому методі аналіз виявлення фальсифікації у деякій частині ЦЗ проводився візуально, що не дозволяло автоматизувати роботу програми. Тому однією із поставлених задач є визначення параметру для відділення фальсифікованої частини ауді сигналу від оригінальних частин.

В якості такого параметру пропонується використовувати максимальне значення відхилення першої похідної кожної апроксимуючої прямої від інших у ПБС будемо позначати його E_i для i-го

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