дасть змогу зекономити кошти і забезпечити кращий захист інформації, на відміну від використання технічних методів захисту.

1. Будз Б.Д., Дудикевич В.Б. Приховані канали витоку інформації з використанням програмованих ПЕМВН // Науковий журнал Східноукраїнського національного університету імені Володимира Даля. – 2010.№ 2(4). 2. Колєсніков С., Будз Б. Дослідження і аналіз ПЕМВ відеоадаптера: матер. І Міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем". – Львів, 2000. – С. 162–163.

УДК 004.932.2

О.В. Наріманова
ОНПУ, м. Одеса

ДОСЛІДЖЕННЯ ЦИФРОВОГО ЗОБРАЖЕННЯ НА НАЯВНІСТЬ ФАЛЬСИФІКАЦІЇ

Запропоновано новий підхід до виявлення та локалізації фальсифікації цифрових зображень без додаткової інформації, що ґрунтується на аналізі збурень максимальних сингулярних чисел блоків 8x8 матриці зображення.

Ключові слова: цифрове зображення, сингулярне число, фальсифікація, коефіцієнти дискретного косинусного перетворення, квантування.

In this paper we propose a new approach to digital images forgery detection and localization without any additional information. It is based on analysis of perturbation of maximum singular values of blocks 8x8 of the image matrix.

Keywords: digital image, singular values, falsification, discrete cosine transform coefficients, quantization.

Вступ

У сучасних умовах масового поширення засобів електронної обчислювальної техніки та можливостей несанкціонованих дій над інформацією виникає необхідність захисту не тільки державної та військової, але й промислової, комерційної та фінансової таємниць. Захист інформації загалом й захист інформації в автоматизованих системах зокрема, стає усе актуальнішою й складнішою проблемою, для вирішення якої необхідна побудова загального системного комплексного підходу до захисту інформації. До недавнього часу комплексні системи захисту інформації були орієнтовані на захист інформації, що створюється, змінюється та передається безпосередньо у самій системі. Проте існування будь-якої системи неможливе без комунікації із зовнішнім середовищем та іншими системами. Отже, захищеність інформації всередині системи залежатиме від достовірності інформації, що надходить до системи ззовні, що призводить до необхідності створення методів перевірки цілісності вхідної для системи інформації. Тому завдання виявлення фальсифікації цифрових сигналів загалом та цифрових зображень (ЦЗ) зокрема, є однією з найважливіших сьогодні завдань в області захисту інформації.

До основних недоліків існуючих у відкритих джерелах методів виявлення фальсифікації ЦЗ можна зарахувати значну обчислювальну складність та необхідність додаткової інформації для проведення аналізу ЦЗ (як правило, характеристик технічних приладів, на яких ЦЗ було створено).

Більшість сучасних цифрових фотокамер використовують для збереження ЦЗ формат JPEG з втратами інформації, що ґрунтується на дискретному косинусному перетворенні (ДКП) або вейвлет-перетворенні. Не обмежуючи спільності міркувань, для визначеності розглядається формат JPEG, що ґрунтується на ДКП. Більшість несанкціонованих змін фотографії зводиться до заміщення

деякої її області в область іншого ЦЗ, що могло бути також отримане після попереднього стиснення JPEG, або зберігалося у форматі без втрат інформації. Після такої фальсифікації отримане зображення зберігається знову у форматі JPEG або з використанням форматів без втрат інформації.

Мета роботи – розробити новий практичний підхід до виявлення та локалізації фальсифікації цифрового зображення без наявності додаткової інформації.

Дослідження цифрового зображення на наявність фальсифікації, що ґрунтується на аналізі коефіцієнтів дискретного косинусного перетворення

В [1] запропонований метод виявлення та локалізації фальсифікації ЦЗ, що були створені із використанням формату JPEG, на основі аналізу функції (1) квадрата середньоквадратичного відхилення значень коефіцієнтів дискретного косинусного перетворення (ДКП) матриці ЦЗ від їх повторно відквантованих значень:

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

де n – кількість блоків 8×8 у ПБС ЦЗ; f_i – коефіцієнт ДКП *i*-го блока 8×8 ПБС ЦЗ, що відповідає заданій частоті (усього 64 частоти); f_i^q визначається за формулою

$$f_i^q = \left[\frac{f_i}{q} \right] q , \; q \in [1,100] .$$

Для підвищення ефективності аналізу в [1] було запропоновано розбити матрицю ЦЗ на т. зв. підблоки сигналу (ПБС) [2] та аналізувати кожен ПБС окремо. Таке попереднє розбиття матриці ЦЗ дає змогу порівняти результати аналізу різних частин цифрового зображення, тобто виявити “нормальну” для цього зображення поведінку функції (1): локальні мінімуми, наявність та кількість областей порушення монотонного зростання функції тощо. Відхилення від “норми” поведінки функції в одному чи кількох ПБС свідчить про наявність у них фальсифікованих областей. Виявлення областей фальсифікації (у разі їх наявності) в одному чи кількох ПБС локалізує область порушення цілісності у самому цифровому зображенні.

Обчислювальні експерименти підтвердили ефективність використання цього підходу до виявлення фальсифікації цифрових зображень, що були первісно збережені у форматах із втратою інформації. Проте зазначений метод має деякі недоліки, оскільки:

1. Аналіз 64-х коефіцієнтів ДКП призводить до значної обчислювальної складності.
2. Метод, що ґрунтується на аналізі повторно відквантованих коефіцієнтів ДКП, під час подальших досліджень не може бути адаптований для цифрових зображень, що зберігаються у форматах без втрати інформації.

Зазначені недоліки зумовлені вибором як параметрів, що досліджуються, коефіцієнтів ДКП матриці ЦЗ. Проте знаходження та дослідження параметра, що однозначно характеризує ЦЗ і не пов’язаний із форматом, у якому воно збережене, може усунути вказані недоліки.

Дослідження цифрового зображення на наявність фальсифікації, що ґрунтується на аналізі сингулярних чисел

Одними з параметрів, що однозначно характеризують матрицю, є сингулярні числа [3]. Для зменшення обчислювальної складності процесу аналізу ЦЗ та можливості подальшої адаптації методу для ЦЗ, що збережені у форматах без втрат інформації, у цій роботі запропоновано замість аналізу $G(q)$ для 64 значень коефіцієнтів ДКП аналізувати функцію $F(q)$ квадрата збурення максимальних сингулярних чисел блоків 8x8 ПБС ЦЗ після повторного квантування коефіцієнтів ДКП за формулою (2):

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

де l_i – максимальне сингулярне число *i*-го блока 8×8 ПБС ЦЗ; l_i^q – максимальне сингулярне число *i*-го блока 8×8 ПБС ЦЗ після повторного квантування зі значенням кроку квантування q; q – крок квантування, що визначає матрицю коефіцієнтів квантування [4], $q \in [1,100]$.

Вибір залучення до аналізу тільки максимальних сингулярних чисел блоків 8×8 зумовлений їх високою стійкістю до збурювальних дій, таких як шуми, що можуть виникнути як під час передачі інформації, так і під час редагування ЦЗ. Окрім того, аналіз лише одного сингулярного числа замість восьми знижує обчислювальну складність розрахунків. Враховуючи вищенаведене, можна перейти до побудови алгоритму виявлення та локалізації фальсифікації на основі аналізу збурення сингулярних чисел матриці ЦЗ.

Алгоритм виявлення та локалізації фальсифікації цифрового зображення

Однією з переваг методу [1] є наочність отриманих результатів аналізу ЦЗ: графік апроксимованої функції $G(q)$ для фальсифікованого ПБС, візуально відділений від графіків ПБС, що відповідають незміненим частинам ЦЗ. Під час побудови алгоритму виявлення та локалізації фальсифікації ЦЗ на основі аналізу сингулярних чисел для збереження наочності також будуватимемо графік апроксимації для функцій $F(q)$ для кожного ПБС матриці ЦЗ.

Основні кроки алгоритму наведені нижче:

1. Розбити матрицю ЦЗ на m ПБС.
2. Для i-го ПБС, $k \in [1, m]$:
   a) для $q_l \in [1,100]$:
      i. сформувати матрицю коефіцієнтів ДКП Q_l за такою формулою:

$$Q_l(i, j) = (1 + (1 + (i - 1 + j - 1))q_l);$$

      ii. провести повторне квантування коефіцієнтів ДКП матриці ПБС за допомогою матриці Q_l;
      iii. розбити матрицю ПБС на блоки 8x8 та отримати значення функції $F_k(q_l)$ за формулою (2);
   б) за отриманими значеннями $F_k(q_l)$ за допомогою методу найменших квадратів побудувати графік функції $\overline{F_k}(q)$.

Пряма функції $\overline{F_k}(q)$, $k \in [1, m]$, що відповідає фальсифікованому ПБС, візуально відділена від прямих інших підблоків.

Результати обчислювального експерименту

Оскільки значення сингулярних чисел відображають лінійну залежність стовпців матриці, можна припустити, що за заміни деякої частини матриці на частину матриці, що відповідає іншому зображенню, збурення сингулярних чисел буде більшим, ніж за заміни на частину тієї самої матриці. Тому під час проведення обчислювального експерименту разом з оригінальними ЦЗ використовувалися фальсифіковані трьома різними способами ЦЗ:

1) деяка частина ЦЗ замінювалася на частину іншого ЦЗ;
2) деяка частина ЦЗ замінювалася на іншу частину цього самого ЦЗ;
3) деяка частина ЦЗ замінювалася своїм дзеркальним відображенням.

На рис. 1, 2 показано характерні результати аналізу оригінального та фальсифікованого ЦЗ на наявність фальсифікації відповідно.

Як бачимо з рис. 1, 2, графіки функцій $\overline{F_k}(q)$ для різних ПБС оригінального зображення візуально невідділені один від одного на відміну від графіка функції $\overline{F_k}(q)$, що відповідає фальсифікованому ПБС, який візуально добре відділений від інших графіків.

Отримані результати обчислювального експерименту дають змогу стверджувати, що запропонований у цій роботі підхід є ефективним у використанні.

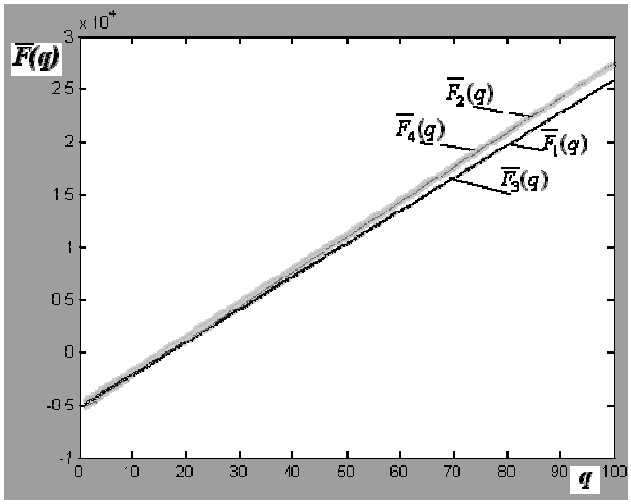

Рис. 1. Результат аналізу оригінального цифрового зображення. Кількість ПБС становить 4

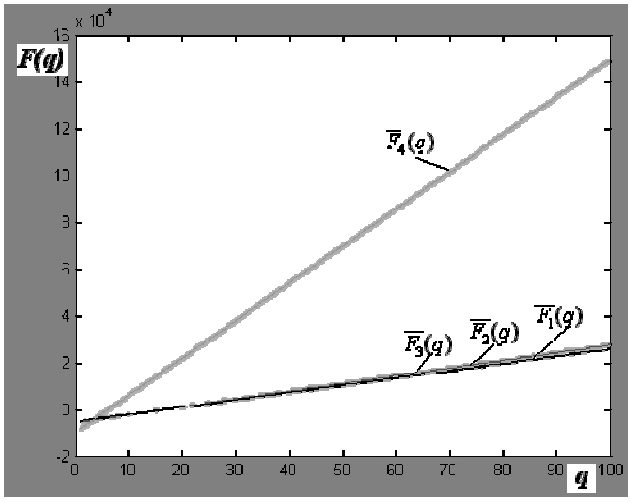

Рис. 2. Результат аналізу фальсифікованого цифрового зображення. Кількість ПБС становить 4, фальсифікація знаходиться у 4-му ПБС

Основними перевагами цього підходу є такі:

1. Для проведення аналізу ЦЗ на наявність фальсифікації потрібне тільки саме ЦЗ без жодної додаткової інформації.

2. Під час виявлення фальсифікації в одному з ПБС ЦЗ одночасно відбувається локалізація області фальсифікації без додаткового дослідження.

3. Цей підхід дає змогу виявити фальсифікацію малих розмірів (порівняних з розмірами блоків 8×8).

4. Окрім вищевказаних переваг 1–3 підходу [1], запропонований у цій роботі новий підхід є простішим з точки зору обчислювальної складності (замість 64 коефіцієнтів ДКП аналізується тільки максимальне сингулярне число блока 8×8);

5. Аналіз сингулярних чисел під час аналізу ЦЗ дає можливість подальшої адаптації розробленого підходу для ЦЗ, що первісно збережені у форматах без втрат інформації.

Висновок

У результаті досліджень, проведених у цій роботі, виявлені особливості поведінки функції квадрата збурення максимальних сингулярних чисел блоків 8×8 ПБС ЦЗ після повторного квантування коефіцієнтів ДКП з різними значеннями кроків квантування як для оригінальних, так і для фальсифікованих ЦЗ. Розроблено новий підхід до виявлення і локалізації фальсифікації ЦЗ на

основі аналізу сингулярних чисел блоків 8×8 ПБС матриці цифрового зображення, який дає змогу ефективно визначати область фальсифікації, тим самим не лише визначаючи наявність, але й локалізуючи її (завдяки розбиттю матриці ЦЗ на ПБС). Проведений обчислювальний експеримент підтверджує ефективність використання запропонованого підходу.

Подальша робота буде спрямована на адаптацію цього підходу для виявлення та локалізації фальсифікації для ЦЗ, що первісно збережені у форматі без втрати інформації.

1. Нариманова Е.В., Чумаченко Ю.В. Обнаружение и локализация фальсификации цифрового изображения в различных условиях её проведения//Додаток до журналу "Холодильна техніка і технологія". – 2011. – №5 (133). – С.41 – 42. 2. Нариманова Е.В. Практическое использование DQ-эффекта для построения универсального метода обнаружения фальсификации ЦС // Вісник Східноукр. нац. ун-ту ім. В. Даля. – 2010. – С.80 – 85. 3. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. – 430 с. 4. Гонсалес Р., Вудс Р. Цифровая обработка изображений.– М.: Техносфера, 2005.– 1072 с.

УДК 004.932.2

К.О. Трифонова
ОНПУ, м. Одеса

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ "COPYPASTE" У ЦИФРОВЕ ЗОБРАЖЕННЯ

Запропоновано спосіб підвищення ефективності методу виявлення та локалізації несанкціонованого втручання "copypaste", що ґрунтується на аналізі сингулярних чисел відповідної матриці.

Ключові слова: фальсифікація, локалізація, ідентифікація, квантування, сингулярні числа.

The way of increasing the efficiency of digital image detection and localization of unauthorized interference "copypaste" method based on analyzing the singular numbers of the corresponding matrix.

Key words: falsification, localization, identification, quantification, singular number.

Вступ

Процес впровадження нових інформаційних технологій в усі сфери життя суспільства неможливий без вирішення питання інформаційної безпеки, складовою частиною якого є завдання визначення автентичності цифрових зображень, створення методів для виявлення несанкціонованого втручання.

Важливість задачі для сучасності змушує багатьох учених шукати шляхи та методи її розв'язку, спираючись на техніку цифрових водяних знаків [1], техніку, що ґрунтується на місцеположенні джерела світла за генерації цифрового зображення [2], ідентифікації цифрового пристрою, за допомогою якого було створено цифрове зображення тощо [3, 4]. Методи, інформація про які доступна з відкритого джерела, ніяк не пов'язані між собою, часто не мають чіткого математичного обґрунтування отриманих результатів, не представляють цілісного апарата, який би ґрунтувався на єдиній математичній базі. Усе це змусило шукати принципово нові математичні інструменти та підходи до розв'язку поставленої задачі загалом, результатом чого став