УДК 004.056

д.т.н, професор Зайцев В.Г., магістрант Шакалов Ю.В.

**Національний технічний університету України
«Київський політехнічний інститут»**

АЛГОРИТМ ЗАХИСТУ JPEG-ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

Abstract

Volodymyr Zaitsev, prof., DcS., Yuri Shakalov, student
JPEG-image protection algorithm using digital watermarking

This paper is dedicated to JPEG-image protection using a digital watermark. The purpose and vital shaping features of such a protection are discussed, as well as an algorithm using round-off errors during quantization stage of JPEG-compression for storing a digital watermark as a unique identifier of an image is proposed. Further improvements are speculated too.

Вступ

Подання зображень чи відео у цифровому вигляді має багато переваг над традиційними способами, як-от: відбиток на папері чи кіноплівка. Цифрові зображення легко і недорого копіювати, простіше розповсюджувати. З іншого боку, ця легкість створення копій цифрових даних робить складнішим дотримання авторських прав. Зі зростанням популярності цифрових зображень і відео виникає нагальна необхідність системи їх захисту від несанкційованого копіювання.

Такий захист можна забезпечити додаванням цифрової мітки (водяного знаку) до даних. Ця мітка має унікально ідентифікувати власника авторських прав та дозволяти відстежити розповсюдження конкретної копії.

Постановка задачі

Задача полягає у визначенні необхідних параметрів захисту JPEG-зображень та розробці алгоритму їх захисту за допомогою цифрових водяних знаків.

Властивості ЦВЗ

Ефективний цифровий водяний знак(ЦВЗ) мусить мати наступні

властивості [1][2]:

- Непомітність: цифрові водяні знаки не можуть погіршувати якість зображення, що захищають;
- Стійкість: видалення цифрового водяного знаку без значного погіршення якості зображення має бути складним (якщо не неможливим). Зокрема, цифровий водяний знак має бути стійким до наступних маніпуляцій із зображенням:
  - загальні операції з обробки сигналу, як-от додавання шуму, зміна яскравості, зміна контрасту та переквантизація;
  - загальні геометричні викривлення, як-от переміщення, маштабування, поворот і кадрування;
  - домовленість кількох користувачів, що володіють одним і тим самим зображенням з різними цифровими водяними знаками з метою їх видалення.

Для використання цифрового водяного знаку у критичних до швидкодії випадках його додавання до даних має бути ефективним. Наприклад при відеомовленні наживо, додавання ЦВЗ до кожного кадру має суттєво не впливати на затримку обробки відеосигналу.

JPEG-ущільнення

JPEG означає "Joint Photographic Expert Group" (Об’єднання експертів фотографії) [3]. Це дуже поширений стандарт ущільнення зображень. Розглянемо його етапи:

1. DCT (англ. Discrete Cosine Transform, дискретне косинусне перетворення) [3] кожного блоку 8x8: спочатку зображення розбивається на блоки 8x8 пікселів, і для кожного блоку виконується DCT. Результатом DCT є набір 64 DCT-коефіцієнтів. Коефіцієнт з нульовою частотою називається "DC коефіцієнт" а 63 інших — "AC коефіцієнти". DC коефіцієнт показує середнє значення блоку зображення. Для чорно-білих зображень він має відношення до загальної яскравості зображення
2. Квантизація: на цьому кроці кожний з 64 DCT коефіцієнтів квантизується за допомогою таблиці квантизації.
3. Зигзагоподібне проходження, RLE, та ентропійне кодування: Квантизовані коефіцієнти реорганізуються у зигзагоподібному порядку та кодуються за допомогою методу RLE (англ. Run Length Encode, кодування повторів) [4]. Нарешті, використовується ентропійне кодування Хафмана (адаптивний

алгоритм оптимального префіксного кодування алфавіту з мінімальною надлишковістю) [4].

Для спрощення пояснення та реалізації алгоритму, всі кроки після квантизації ігноруються. Щоб отримати JPEG-файл після вбудовування цифрового водяного знаку, необхідно виконати кодування Хафмана .

Алгоритм JPEG-ущільнення не дозволяє захист закодованих за його допомогою зображень, тому вимагає створення спеціального алгоритму захисту за допомогою цифрового водяного знаку.

Алгоритми додавання та виявлення ЦВЗ

Під час JPEG-ущільнення, квантизація складається з нормалізації та округлення [3]. Перед округленням можна отримати нормалізоване значення близьке до *.5 (тобто будь-яке значення з дробовою частиною, що близька до 0.5), наприклад, якщо DCT коефіцієнт дорівнює 22 і відповідний рядок таблиці квантизації дорівнює 4, тоді як нормалізоване значення отримаємо 5.5. За застосування звичайного округлення результатом буде 6, однак насправді округлення до 5 чи до 6 не дуже сильно впливає на якість зображення. Цю властивість можна використати для вбудовування цифрового водяного знаку.

Необхідно точно визначити поняття "близько до *.5" перед детальним поясненням алгоритму, що в свою чергу вимагає компромісу між стійкістю та якістю. Припустимо, що [*.5-*a*, *.5+*a*] є проміжком, близьким до *.5. Чим більший проміжок, тим більше значень можна використовувати для збереження водяного знаку, але тим менша якість захищеного зображення. Користувач може вибрати необхідне значення з урахуванням своїх вимог застосування зображення. Було вирішено не використовувати DC-коефіцієнти, щоб водяний знак був стійкий до змін яскравості зображення.

Для зручності введемо наступні терміни:

Файл позиціювання — це файл, що містить всю необхідну інформацію про те, де розміщувати водяний знак у відповідному зображенні.

Файл-основа — це файл, що містить зображення із фіктивним водяним знаком, тобто з таким, що всі його біти є нулями. Він служить основою для вбудовування реального водяного знаку бо одиничні біти можуть бути записані простим додаванням одиниці до відповідного біта файлу-основи.

Алгоритм додавання ЦВЗ

Алгоритм додавання ЦВЗ може бути розділений на два етапи:

1. Підготовка. На вхід подається оригінальне зображення і параметр a,

яке перетворюється у файл-основу. Під час квантизації за допомогою параметру a визначаються та зберігаються у файл позиціювання всі позиції, де може бути записаний біт ЦВЗ, а потім в них вставляються нулі.

2. Додавання ЦВЗ. На вхід подаються файл позиціювання, файл-основа, і деяка бітова послідовність, що слугуватиме власне ЦВЗ. Виконуються такі кроки:
   1. Застосування коду з корекцією помилок до бітової послідовності ЦВЗ
   2. Закодована послідовність вбудовується у файл-основу на позиціях, збережених у файлі позиціювання.
   3. Повторення закодованого ЦВЗ доки всі позиції будуть використані.
   4. Завершення JPEG-ущільнення.

Алгоритм виявлення ЦВЗ

Алгоритм складається з п’яти етапів:

1. Нівелювати можливі геометричні викривлення зображення за допомогою афінних перетворень.
2. Отримати необроблені ЦВЗ дані із зображення за допомогою файлу-основи та файлу позиціювання, створених при записі ЦВЗ у файл.
3. Виконати нормалізацію отриманих значень, оскільки у деяких позиціях можуть трапитись значення, відмінні від 0 чи 1. Перетворення відбувається наступним чином: якщо $b <= 0$ тоді $b=0$ інакше $b=1$.
4. Відновити ЦВЗ за допомогою мажоритарного правила, аналізуючи всі отримані бітові послідовності ЦВЗ.
5. Застосувати декодування з корекцією помилок і виявити ЦВЗ.

Висновки

Запропоновано метод захисту JPEG-зображень за допомогою ЦВЗ, що використовує помилки округлення під час етапу квантизації JPEG-ущільнення. За результатами експериментальних досліджень, якість захищених зображень не гірша, ніж звичайних JPEG- зображень. ЦВЗ є досить стійким до операцій з обробки сигналу (зміна яскравості та контрасту, гамма корекції, подальше ущільнення) та геометричних викривлень (масштабування, поворот). Більш того, вбудовування водяного знаку є дуже ефективним, бо відбувається під час ущільнення зображення і перед ентропійним кодуванням, тому метод може бути використаний при відео-мовленні наживо.

Описаний метод може бути легко застосований до відео, стисненого за MPEG алгоритмом. Ідея приховування інформації у помилках округлення також може бути застосована з будь-яким способом ущільнення, що має етап квантизації, включаючи навіть деякі методи аудіо-ущільнення. Можливими покращеннями методу є вдосконалена протидія домовленості користувачів з метою видалення водяного знаку, а також така модифікація декодерів JPEG, яка заборонить читання файлів з недійсним водяним знаком.

Література

1. *Kumar M.* Steganography and Steganalysis of JPEG Images. University of Florida Journal. January 2011, pp. 32-39
2. *Грибунин В., Оков И., Туринцев И.* Цифровая стеганография. – СПб: Солон-Пресс, 2002. – 277 с., ил.
3. ITU CCIT T-81. Information technology digital compression and coding of continuous-tone still images requirements and guidelines. September 1992.
4. *Malek M.* Coding Theory. California State University Journal. October 2004, pp. 17-24.