УДК 004.054

Є.С.Мельник
О.Ю.Софина

Реалізація методу створення водяних знаків на зображеннях з метою захисту авторських прав

Вінницький національний технічний університет

Анотація
Реалізовано методи реалізації водяних знаків з метою захисту авторських прав за допомогою бібліотек на мові Python – метод дискретного косинусного перетворення, ліфтингового вейвлет-перетворення та сингулярного розкладу.
Ключові слова: водяні знак, алгоритми, бібліотеки на мові Python.

Abstract
The methods of implementing copyright protection watermarks using Python libraries have been implemented - the method of discrete cosine transformation, lifting wavelet transformation and singular decomposition..
Keywords: watermarks, algorithms, libraries in the Python language.

Вступ

Водяні знаки є ефективним інструментом для захисту цифрових зображень від незаконного використання та несанкціонованої поширення.

Метою роботи є детальне дослідження алгоритмів побудови водяних знаків та їх реалізація з використанням бітових рядків у мові програмування Python [1].

Цифровий водяний знак - це вбудований сигнал, що постійно присутній у цифрових даних, таких як аудіо, зображення, відео та текст. Він може бути виявлений або видобутий за допомогою обчислювальних операцій, що дозволяє підтвердити їх автентичність.

Результати дослідження

Дослідження в області дискретного вейвлет-перетворення є менш популярними порівняно з дослідженнями в області дискретного косинусного перетворення. Одна з причин цього полягає у тому, що дискретне косинусне перетворення широко використовується у форматі JPEG, тоді як вейвлет-перетворення зазвичай використовується у форматі JPEG2000. Однак, сучасні дослідження показують, що стеганографічні методи, основані на вейвлет-перетворенні, У дослідженні, проведеному Г.В. Ахмаметьєвою та Г.А. Баранюк, було досліджено метод вбудови цифрового водяного знаку в зображення на основі вейвлет-перетворення. Цей метод демонструє високу стійкість до різних видів атак, а також здатність зберігати якість навіть при стисненні у форматі JPEG. Він також показав високу точність детектування цифрового водяного знаку навіть у випадку наявності різних атак, таких як накладання фільтрів, шуми та афінні перетворення [2]. Метод ґрунтується на декількох кроках, включаючи вейвлет-перетворення синьої складової сигналу контейнера, перетворення цифрового водяного знаку в полутонове зображення та вбудовування його в деталізовані коефіцієнти вейвлет-перетворення. Результати показали дуже високу вірогідність детектування цифрового водяного знаку, навіть при сильному стисненні. У науковому дослідженні Д. Бабі та Д. Томаса була запропонована техніка захисту даних, яка використовує дискретне вейвлет-перетворення для приховування кількох кольорових зображень в одному контейнері. Цей метод передбачає застосування вейвлет-перетворення до кольорових матриць зображення-контейнера, подальшу обробку діапазону LL та вбудовування

інформації зі секретних зображень в різні області контейнера. Результати цього методу були досить задовільними, але не були перевірені на стійкість до атак та вплив на візуальну якість зображення. У роботі Б. Сінга було запропоновано новий підхід до стеганографії зображень, спрямований на підвищення візуальної якості стеганоповідомлення. Деталі цього підходу не наведені, але вказується, що він пропонує новий метод для стеганографії зображень[3].

В даній роботі було запропоновано метод стеганографії зображень, в якому контейнер розкладається з використанням дискретного вейвлет-перетворення (ДВП) з метою отримання вейвлет-піддіапазонів. Для кожного високочастотного вейвлет-піддіапазону обчислюється порогове значення. Для вбудовування секретного зображення в стеганоповідомлення запропоновано використовувати напівшістнадцятковий код (SHC), що дозволяє перетворити значення пікселів секретного зображення на менші еквівалентні значення, що мінімізує спотворення зображення стеганоповідомлення. Один з недоліків цього методу полягає у відсутності досліджень щодо стійкості до атак і детектування додаткової інформації. Інший метод, запропонований в статті "High PSNR based Image Steganography" індійського вченого Н. Сінга, використовує ліфтингове вейвлет-перетворення (LWT), дискретне косинусне перетворення (ДКП) та сингулярний розклад коефіцієнтів ДКП для вбудовування секретної інформації. Цей метод може застосовуватись як до зображень, так і до відео-файлів. В основі методу лежать кроки, такі як розбиття контейнера на блоки, застосування ДКП та LWT до блоків, а також вбудовування ЦВЗ в матрицю сингулярних чисел. Цей метод показав високі результати, зокрема показник пікового відношення "сигнал/шум" досягає 51 дБ. Однак, ця стеганографічна система є напівзакритою, що означає, що для вилучення додаткової інформації потрібно мати оригінальний ЦВЗ. Останнім часом було розроблено новий метод стеганографії, який не потребує оригінального контейнера або ЦВЗ для вилучення додаткової інформації. Результати цього методу є кращими, ніж результати, описані в роботі "High PSNR based Image Steganography". В цьому методі використовуються пари вейвлет-фільтрів, які можуть перетворюватися в первинну та подвійну послідовність підйому для підняття програми. На рисунку 1 показано приклад 2-рівневого вейвлет-перетворення зображення. Поліфазна матриця фільтра 9/7 для ефективного виробництва така:

$$W(x) = \begin{bmatrix} 1 & a(1+x^{-1}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ d(1+x) & 1 \end{bmatrix} \begin{bmatrix} 1 & c(1+x^{-1}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} K & 0 \\ 0 & 1/K \end{bmatrix} \quad (1.1)$$

де a, b, c, d — чотири параметри підйому, а K — параметр масштабування

Рисунок 1 – Результат отриманий вбудовою ЦВЗ в зображення

Висновки

Отже, розроблений метод забезпечує високу якість заповненого контейнеру, високу пропускну здатність прихованого каналу зв'язку та високий рівень подібності між вбудованим і вилученим ЦВЗ. Крім того, він майже нечутливий до різних видів атак і може бути ефективно використаний у практичних застосунках..

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Посібник по Python. URL: https://docs.python.org/uk/3/tutorial/index.html (дата звернення: 20.04.2023)
2. Обзор застосування вейвлет-преобразования в задачах інтелектуального аналізу URL: http://dspace.nbuv.gov.ua/handle/ (дата звернення: 20.04.2023)
3. Secure transmission of data using image steganography. URL: https://nevonprojects.com/secure-data-transfer-over-internet-using-image-steganography/ (дата звернення: 20.04.2023).

Мельник Євгеній Сергійович — студент групи 1АКІТ-19б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: zheps14@gmail.com

Науковий керівник: ***Софина Ольга Юріївна*** — к.т.н., доцент кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: sofyna.o.y@vntu.edu.ua

Melnyk Yevhenii Serhiyovych — student of group 1AKIT-19b, faculty of intellectual information technologies and automation, Vinnytsia National Technical University, Vinnytsia, e-mail: zheps14@gmail.com

Supervisor: ***Sofina Olga Yuriivna –*** Associate Professor of Automation and Intelligent Information Technologies Department, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: sofyna.o.y@vntu.edu.ua