УДК 004.056.53

Н. В. Копайгородська
В. В. Карпінець

МЕТОДИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ ТА ВИКОРИСТАННЯ ЦИФРОВИХ ЗОБРАЖЕНЬ В ОНЛАЙН-СЕРВІСАХ

Вінницький національний технічний університет

Анотація.
Досліджено стеганографічні методи захисту від несанкціонованого копіювання та використання. Проаналізовано основні недоліки та переваги існуючих методів для вирішення задачі захисту зображень в онлайн-сервісах.
Ключові слова: стеганографія, авторське право, несанкціоноване копіювання та використання, цифрові водяні знаки.
Abstract
Steganographic methods of protection against unauthorized copying and use have been investigated. The main disadvantages and advantages of existing methods for solving the problem of image protection in online services are analyzed.
Keywords: steganography, copyright, unauthorized copying and use, digital watermarks.

У зв'язку з бурхливим розвитком мультимедійних технологій постає питання захисту авторського права творів в цифровому вигляді, особливо зображень. Доступ до фотографій настільки великий та легкий, що число незаконного використання фотографічних творів іншими особами щоразу стає більшим, а це свідчить про порушення авторського права. Широко використовуються онлайн-сервіси, веб-сервіси у наш час. Відповідно це дає змогу незаконно скопіювати, та повторно завантажити зображення, порушуючи авторське право [1]. Цифровий водяний знак (ЦВЗ) технологія, створена для захисту авторських прав мультимедійних файлів. ЦВЗ поділяються на видимі і невидимі. Зазвичай цифрові водяні знаки невидимі. Зазвичай ця інформація є текстом або логотипом, який ідентифікує автора . Більш стійкими до різного роду спотворень та компресії є методи другої групи. До відомих методів відносяться методи на основі використання дискретного косинус перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення [2]. Таким чином було розглянуто існуючі методи захисту зображень за допомогою цифрових водяних знаків, виявлено їх головні переваги та недоліки. Проведено порівняльний аналіз даних методів вбудовування цифрових водяних знаків в зображення.

Алгоритм Куттера-Джордана-Боссена є одним з найбільш ефективних методів вбудовування інформації в зображення. Він полягає у вбудовуванні до каналу синього кольору RGB зображення, оскільки саме до нього с найменш чутливою система людського зору. Також, пропонується модифікація алгоритму на основі трьох складових кольору для підвищення стійкості алгоритму до різних видів атак, а також збільшення обсягу прихованою інформації в роботі [3].

Перевагою цього методу є висока пропускна здатність, стійкість до несанкціонованого ознайомлення, до частотного детектування, до руйнування молодшого біта контейнера та до атак стискання. Недоліком є те, що вилучення повідомлення має імовірнісний характер. Для зменшення імовірності помилки використовується завадостійке кодування. Також можна у процесі вбудовування кожен біт повторювати декілька разів (багаторазове вбудовування).

Метод Коха-Жао один з найпоширеніших на сьогодні методів приховання конфіденційної інформації в частотної області зображення полягає у відносній заміні величин коефіцієнтів дискретно косинусного перетворення (ДКП) [4].

Перевагами методу є: використання частотної області, важкість випадкового знаходження ЦВЗ, легкість виявлення порушень. До недоліків можна віднести: важкість реалізації, низька пропускна здатність.

Метод Бенгама-Мемона-Ео-Юнга є модифікацією методу Коха та Жао. Оптимізація методу Коха-Жао виконана за двома напрямками:

1) Для вкраплення бітів ЦВЗ було запропоновано використовувати не всі блоки зображення, а тільки ті, які підходять для даної мети;

2) В частотній області блоків зображення як безпосередні носії біта повідомлення обираються не два, а три коефіцієнти ДКП, що дозволяє суттєво зменшити візуальні спотворення стеганоконтейнера [5].

Залежно від заданого завдання, використовуються різні алгоритми. Якщо необхідна перевірка цілісності файлу-зображення, доцільно використовувати алгоритм, що впроваджує крихкий ЦВЗ, якщо необхідно передати секретне повідомлення в файлі-контейнері потрібні вже інші характеристики для ЦВЗ, якщо необхідно підтвердження авторських прав на зображення, необхідний вибір алгоритму, здійснює впровадження стійкого ЦВЗ, стійкого до атак на контейнер [6].

Було здійснено аналіз стійкості методу захисту від несанкціонованого копіювання та використання за таким набором характеристик: пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування та виявлення. Необхідно відзначити хороші показники методів вбудовування у частотну область зображення.

Для порівняльного оцінювання якості стеганографічних засобів було використано загальновідомі показники, що дають кількісні оцінки. Вони оперують із зображеннями на рівні пікселів. Оцінювання проводилось за такими показниками: максимальна різниця, середня абсолютна різниця, якість зображення, співвідношення сигнал/шум, нормована взаємна кореляція. Відповідно до показників і характеристик найбільш стійким є метод Бенгама-Мемона-Ео-Юнга [7].

Отже, було проаналізовано існуючі стеганографічні методи захисту, виявлено їх переваги та недоліки. Більш стійкими до різноманітних спотворень, в тому числі і компресії, є методи, які використовують для приховування даних не просторову область контейнера, а частотну. Виходячи з цих міркувань, для вирішення задачі щодо, захисту цифрових зображень від несанкціонованого копіювання та використання, використовуючи цифрові водяні знаки було обрано метод Бенгама-Мемона-Ео-Юнга.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хорошко В.О. Комп'ютерна стеганографія: [навчальний посібник] / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. – Вінниця : ВНТУ, 2017. – 155 с.
2. Коханович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Коханович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.
3. Грибунин В.Г. Цифровая стеганография. / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М.: СОЛОН-Пресс, 2012
4. Аграновский А.В. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2013. – 152 с.
5. Benham D. Fast Watermarking of DCT-based Compressed Images / D. Benham, N. Memon, B. Yeo, M. Yeung // Proc. of the International Conf. on Image Science, Systems and Technology. – . – Vol 1. – P. 243–252.
6. Ivanenko V.G., Ushakov N.V. Digital watermarks in electronic document circulation. Bezopasnost' informacionnyh tekhnologij, 2017, №3, p. 37-42.
7. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

Копайгородська Наталія Василівна — студентка групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail:natali4ka16@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця.

Kopaihorodska Nataliia Vasylivna — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia

Supervisor: ***Karpinets Vasyl V.*** — Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia.