DOI 10.15276/imms.v10.no1-2.75
УДК 004.056.6

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 75-83

РОЗРОБКА МЕТОДУ КОНТРОЛЮ ЦІЛІСНОСТІ ЗОБРАЖЕННЯ НА ОСНОВІ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

І.С. Чіклікчі, А.А.Смагін, Л.В. Нечитайлова, Н.І. Кушніренко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: infsec2011@gmail.com

Розробка засобів та методів захисту інформаційної цілісності документів, зокрема цифрових зображень, залишається традиційно актуальною задачею. Популярність отримали методи контролю цілісності контенту з використанням прихованих цифрових водяних знаків. Цілісність тут може гарантуватися шляхом хешування файлу. Хеш-суми зображень можуть зберігатися у окремій захищеній базі даних. Для зручності роботи системи бажано, щоб хеш або інший модифікатор, який гарантує цілісність, був вбудований безпосередньо у зображення. Переважна більшість цифрових фотографій зберігається в стисненому вигляді з використанням алгоритмів групи JPEG. Оскільки алгоритм не зберігає точні значення пікселів, додавання цифрового водяного знаку (ЦВЗ) в файли такого типу передбачає додавання інформації в просторі перетворень, іншими словами, зміні підлягають квантовані коефіцієнти дискретного косинусного перетворення (ДКП), саме ті дані, які залишаються незмінними в процесі стиснення зображення. У ролі ЦВЗ виступатиме хеш-сума зображення, яка отримується шляхом використання хеш-функції. В алгоритмах, які працюють з зображенням такого формату, зазвичай змінюються молодші значущі біти (LSB), і інформація впроваджується послідовно. У даній статті розроблено метод контролю цілісності зображення на основі цифрового водяного знаку, який базується на вбудовуванні хеш-суми в найменш помітні місця зображення і дозволяє оцінити психовізуальну помітність впровадження. На етапі перед вбудовуванням проводиться аналіз статистики зображення з метою виявлення найбільш вдалих місць для вбудовування додаткової інформації. Наведені результати обчислювального експерименту.

Ключові слова: контроль цілісності зображень, дискретне косинусне перетворення, цифровий водяний знак, вбудовування секретної інформації, хеш-сума.

Вступ

В еру стрімкого розвитку інформаційних технологій дані, які зберігаються і передаються у цифровому форматі, все частіше потребують захисту від модифікації, несанкціонованого копіювання та використання. Одним із основних видів цифрового контенту на сьогоднішній день є цифрове зображення. Протидія копіюванню зображень, захист авторських прав власників на зображення, захист торгової марки продукції [1] – це далеко не повний перелік напрямків, які сьогодні існують. Крім того, виникає необхідність перевірки інформаційної цілісності зображень з метою виявлення присутності несанкціонованих змін і фальсифікації. Тому на сьогоднішній день розробка засобів та методів перевірки інформаційної цілісності зображення є актуальною задачею. Існуючі методи базуються на різних підходах, кожен з яких має свої переваги та недоліки. Популярність отримали методи контролю цілісності контенту з використанням прихованих цифрових водяних знаків. В такому випадку цілісність зображення може гарантуватися шляхом хешування файлу. Хеш-суми зображень можуть зберігатися у окремій захищеній базі даних. Але для зручності роботи системи бажано, щоб хеш або

інший модифікатор, який гарантує цілісність, був вбудований безпосередньо у зображення.

Мета та задачі роботи

Метою роботи є розробка метода контролю цілісності зображення, який ґрунтується на вбудовування в зображення ЦВЗ, який містить його хеш-значення.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз моделей і методів контролю цілісності зображень;
- запропонувати власний метод контролю цілісності зображень з вбудовування хеш значення;
- розробити програмне забезпечення, яке реалізує запропонований метод контролю цілісності;

Об'єкт дослідження – процеси забезпечення достовірності джерела поширення та контролю цілісності зображення на основі цифрових водяних знаків.

Предмет дослідження – методи контролю цілісності зображень, що ґрунтуються на використанні цифрових водяних знаків.

Основна частина

Для впровадження хеш-значення в зображення існує 4 основних методи[2], три з яких досить прості у реалізації, проте не є надійними. Четвертий метод базується на використані цифрового водяного знаку, що робить цього більш надійним, але і більш складним у реалізації.

Перші три методи контролю цілісності зображень: зберігання хеш-суми поруч з зображенням, зберігання хеш-суми у віддаленій базі даних, поєднання хеш-суми та зображення (наприклад її додавання в кінець зображення не використовуючи жодних стенографічних методів). Мінусом цих методів є надійність. Використовуючи кожен з них, можна легко отримати хеш-суму зображення і в підсумку змінити її, а так само і саме зображення. Таким чином, вони ніяк не можуть гарантувати цілісність зображення, а цей критерій є головним для алгоритму, що розробляється.

Четвертий спосіб контролю цілісності використовує стенографічний метод на основі вбудовуванні непомітного ЦВЗ. В даному випадку зловмисник не зможе зрозуміти, що зображення може підлягати контролю цілісності і будь-яка його модифікація може бути з легкістю виявлена. В даному методі так само використовується хеш-сума зображення, однак пропонується використання самого зображення в якості сховища для хеш-суми (рис.1). Для того щоб вбудувати хеш-суму використовують молодший розряд обраних частотних компонентів зображення. Метод заміни молодших біт (LSB-метод) заснований на тому, що молодші розряди графічних, аудіо та відеоформатів несуть мало інформації і їх зміна практично не позначається на якості переданих зображення [3]. Це дає можливість використовувати їх для приховування конфіденційної інформації. Однак за рахунок введення додаткової інформації спотворюються статистичні характеристики зображення-контейнера і приховане повідомлення легко виявити за допомогою статистичних методів стеганоаналіза, таких як оцінка ентропії і коефіцієнтів кореляції [4].

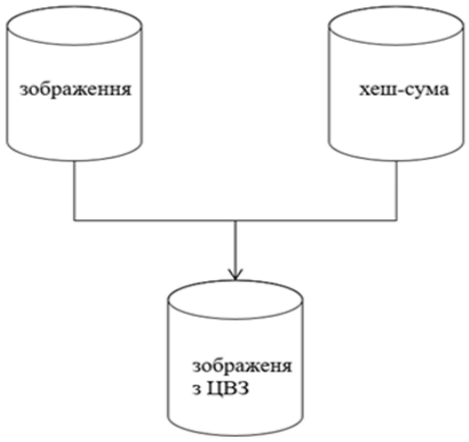


Рис. 1. Використання цифрового водяного знаку

Недолік даного методу полягає в тому, що не завжди можливо помістити у зображення хеш певної довжини. Щоб уникнути цього можна обчислювати кількість пікселів в зображені і підбирати потрібну довжину хешу.

Хеш-функція – це функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованої довжини, так званий «дайджест». Якщо дані зміняться, то і дайджест, також зміниться.

Позначимо хеш-функцію через H, вихідні дані – через T, вхідні дані – через T'. Контроль цілісності даних зводиться до перевірки рівності[5]:

$$H(T') = H(T).$$

Якщо воно виконано, вважається, що $T' = T$.

Збіг дайджестів для різних даних називається колізією – $H(T) = H(Y)$. Колізіїможливі, оскільки потужність множини дайджестів менше, ніж потужність безлічі даних, що підлягає хешуванню. Однак те, що H –одностороння функція, означає, що за прийнятний час спеціально організувати колізію неможливо.

SHA-1, SHA-2 і SHA-3 –це сімейство криптографічних хеш-функції, які відносяться до алгоритмів безпечного хешу (“Secure hash algorithms”)[6]. Вони відрізняються між собою довжиною хеш-суми, яка покращує стійкість до атак. В SHA-1 це 160 бітів, в SHA-2 це 256 бітів і в SHA-3 це 512 бітів, крім довжини хеш-суми у них також різні внутрішні дизайни. Метод контролю цілісності зображення, який пропонується в даній роботі буде використовуватиSHA-1 з довжиною хеш-значення 160 бітів, через наступні переваги:

- складність генерування хеш-суми протягом найближчих років буде неприступною для підбору хеш-суми методом «грубої сили»: завдання знаходження колізій вимагає $2^{160/2} = 2^{80}$ операцій, а завдання знаходження прообразу - початкового повідомлення - по його хешу, вимагає $2^{160/2}$ операцій[7],
- впроваджувальна кількість бітів є оптимальною, тому що лише 160 бітів будуть змінені і це буде збільшувати помилку другого роду для статичних аналізаторів, так як вони залежать від кількості змінених бітів у зображенні.

Стеганографічні методи, що діють в частотної області, зазвичай ховають дані в коефіцієнтах ортоганального перетворення контейнера. Для цього найчастіше

використовуються перетворення, що застосовуються в сучасних алгоритмах стиснення з втратами (дискретне косинусне перетворення в стандарті JPEG і вейвлет-перетворення - в JPEG2000). Розглянемо докладно алгоритм стиснення зображення JPEG на рисунку2.

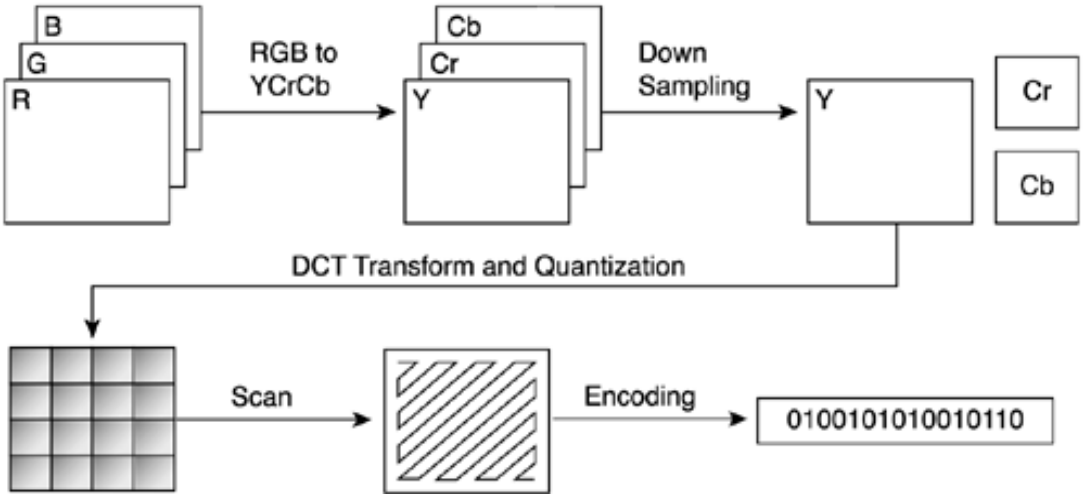


Рис. 2. Алгоритм стиснення зображення формату JPEG

У цьому алгоритмі зображення перетворюється з колірного простору RGB в YCbCr, де Y – компонента яскравості, а Cb і Cr - компоненти кольоровості. Тому важливіше зберегти більшу точність при передачі Y, ніж при передачі Cb і Cr. Значення каналів розбиваються на блоки 8x8. Кожен блок піддається дискретному косинусному перетворенню (ДКП)[8]. Таким чином, при перетворенні виходить матриця, елементи якої відповідають інтенсивності різних просторових частот вихідного блоку. Для кожного елемента матриці дискретного косинусного перетворення існує відповідний елемент матриці квантування. Отримуємо матриця розподілом кожного елемента матриці дискретного косинусного перетворення на відповідний елемент матриці квантування і наступним округленням результату до найближчого цілого числа. Отримана матриця перетворюється в 64-елементний вектор таким чином, що на початку вектора розташовуються коефіцієнти матриці, що відповідають низьким частотам, а в кінці - високим. Отриманий вектор згортається за допомогою алгоритму групового кодування RLE[9], а потім кодується кодами Хаффмана.

Для того щоб записати хеш-суму в зображення спочатку необхідно вибрати для впровадження такі ДКП-компоненти блоків зображення, які будуть найменш помітні. Для того що б їх визначити ми будемо використовувати псіховізуальну модель JPEG, яка заснована на особливостях сприйняття зображень людиною. Зазвичай використовується грубе квантування високочастотної складової зображення і більш акуратне квантування низькочастотної складової, знижуючи тим самим точність передачі різких переходів яскравості і відтінків кольору.

На основі матриці квантування, ми створюємо матрицю індексів, в якій ставимо у відповідність кожному з компонентів ДКП індекс прихованості цього компонента. Таким чином ми отримаємо вектор з цих індексів і їх розташування, вибираємо 160 елементів з найбільшими індексами прихованості, щоб записати хеш-суму.

Основні кроки можна побачити на рисунку 3:

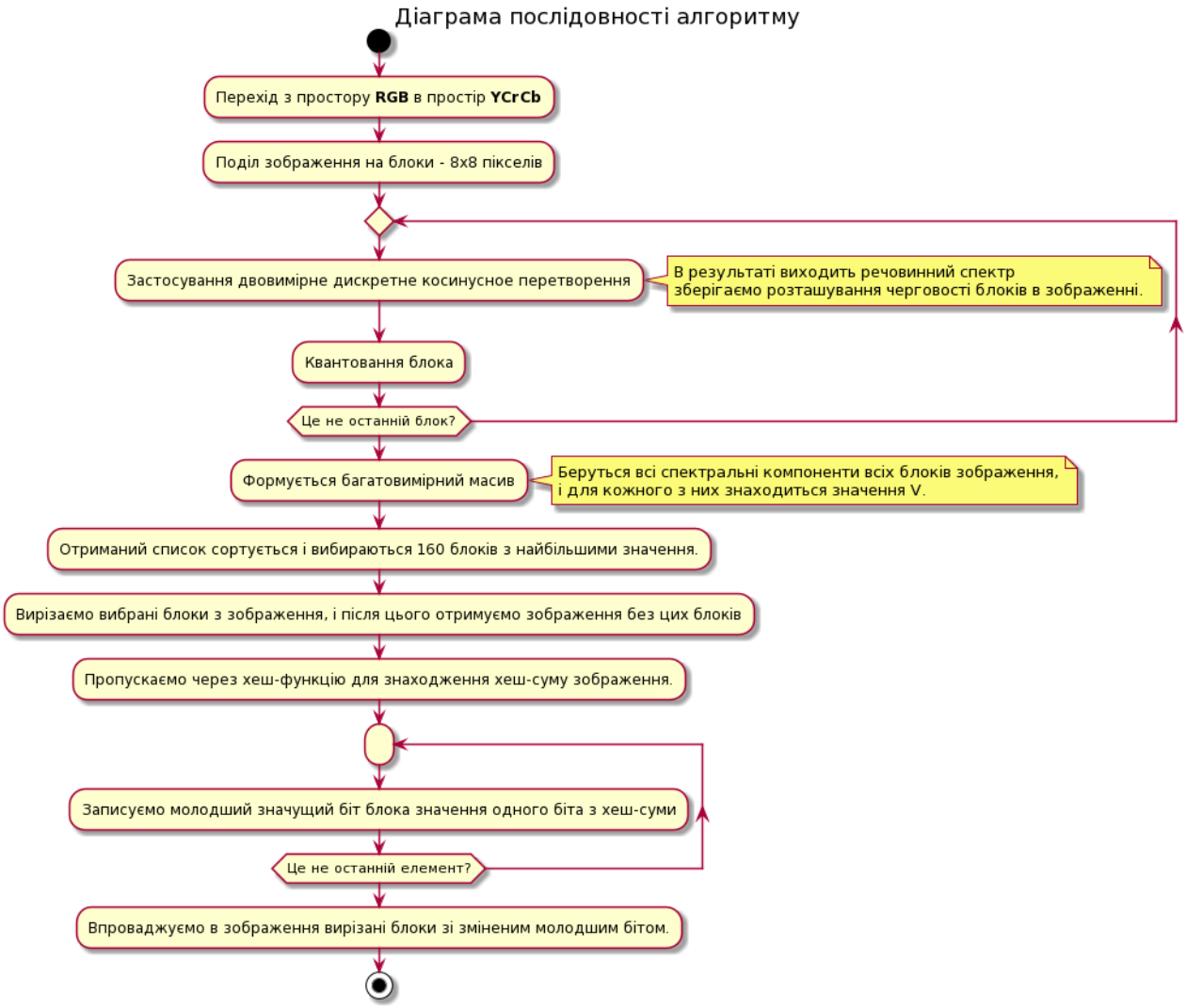


Рис. 3. Алгоритм методу контролю цілісності зображення.

Основні кроки розробленого методу контролю цілісності зображення.

Крок 1. Перехід з простору RGB в простір YCrCb.

Крок 2. Поділ зображення на блоки - 8x8 пікселів.

Крок 3. До кожного блоку застосовується двовимірне дискретне косинусное перетворення. В результаті виходить речовинний спектр.

Крок 4. Сформовані блоки піддаються квантуванню. Далі з них формується багатовимірний масив.

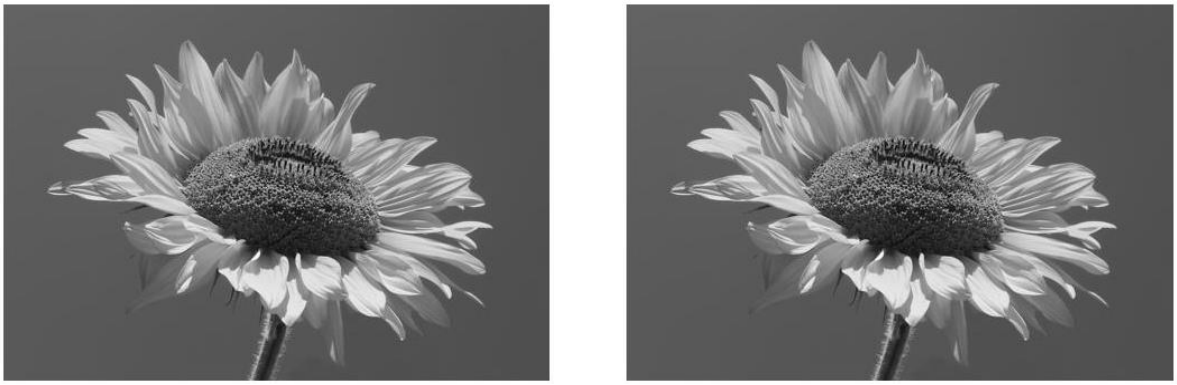
Таким чином, беруться всі спектральні компоненти всіх блоків зображення, і для кожного з них знаходиться значення прихованості. Отриманий список сортується і вибираються 160 блоків з найбільшими значеннями.

Крок 5. Вирізаємо вибрані блоки з зображення, пам'ятаючи їх місце розташування тачерговість блоків в зображенні і після цього отримуємо зображення без цих блоків, яке пропускаємо через хеш-функцію для знаходження хеш-суми зображення.

Крок 6. Знаючи черговість блоків записуємо в кожен молодший значущий біт блока значення одного з бітів хеш-суми. Таким чином ми впроваджуємо хеш-суму в зображення в найбільш непомітні місця.

Крок 7. Додаємо назад змінені вирізані блоки в зображення.Завершується стиснення зображення.

Виконаємо тестування та аналіз результатів роботи розробленого методу. Для експерименту було обрано зображення з роздільною здатністю 340x487 пікселів (рис. 4(а)). Зображення-результат наведені на рисунку 4(б).



а б

Рис. 4. Порівняння оригінального та результуючого зображень: а – оригінальне зображення; б – зображення з вбудованим ЦВЗ

Як видно, на перший погляд, зображення ідентичні. Однак, при виділенні і посилення різниці між зображеннями, можна помітити незначні, відмінності (рис. 5).

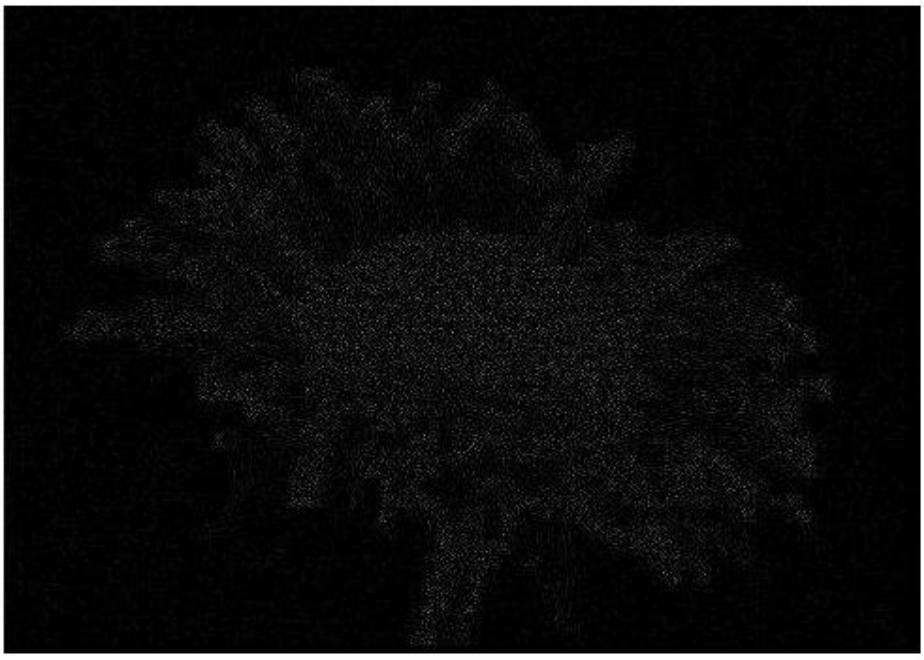


Рис. 5. Різниця між зображеннями

Програмна реалізація запропонованого методу здійснювалася в середовищі Python IDLE.

Для оцінки якості зображення використаємо такі об'єктивні критерії як середньоквадратичний критерій (MSE) та співвідношення «сигнал/шум» - SNR.Для експерименту буде використовуватися група з 10-ти зображень в яких був вже введений

значення хешу. Значенням критерії оцінки буде медіана для цих зображень. MSE для цих зображень складає 3.676. Параметр SNR дозволяє провести аналіз рівня спотворень, які вносяться в контейнер під час приховування в ньому інформації. SNR для цих зображень складає 18.410.

Так само зрівняємо MSE та SNRдля групи початкових зображення в яких не було введено значення хешу. Зменшимо коефіцієнти компресії на 10% від початкової. MSE для цих зображень складає 4.012, SNR – 17.203.

Висновки

У роботі розглянуті основні методи контролю цілісності зображень на основі хеш-значення та проведено їх аналіз. Наведені основні принципи формування зображень формату JPEG. Розроблено метод контролю цілісності зображення на основі цифрового водяного знаку, який використовує у якості ідентифікатора цілісності хеш-значення, отримане шляхом застосування функції SHA-1 до оригінального зображення. На етапі перед вбудовуванням проводиться аналіз статистики зображення з метою пошуку найбільш вдалих місць для вбудовування. Таким чином, впроваджене хеш-значення залишається непомітнім для людського ока.

Список літератури

1. Грібунін В.Г. Кайданів І.М., Туринців І.В. Цифрова стеганографія. Москва: Солон-Прес, 2009. 272 с.
2. Yang C.N., Lin C.C., Chang C.C. Steganography and Watermarking. Nova Science Publishers, 2013. 200 p.
3. Таранчук А.А. Гальпер Л.Г. Стеганографічній метод піховування даних до області частотних перетворень зображення. *Вісник Хмельницького національного університету*. 2009. № 2. С. 197-201.
4. Wang Y., Moulin P. Steganalysis of block-DCT image steganography Urbana, USA: University of Illinois at Urbana-Champaign,2010.172 p.
5. Хеш-функція – картка даних терміну. Українське агентство зі стандартизації. URL:uas.org.ua/ua/bank-danih/natsionalniy-bank-terminiv/znachennya-termina/?term-id=38741.
6. Stevens M., Bursztein E., Karpman P., Albertini A, Markov Y., Katz J., Shacham H. The First Collision for Full SHA-1. 2017. 76c. URL: web.archive.org/web/20180515222208/ http:/shattered.io/static/shattered.pdf.
7. NIST Comments on Cryptanalytic Attacks on SHA-1. URL: csrc.nist.gov/groups/ST/hash/ statement.html.
8. Фисенко В.Т., Фисенко Т.Ю. Компьютерная обработка и распознавание изображений. СПб: Санкт-Петербургский государственный университет информационных технологий, механики и оптики, 2009. 192 с.
9. Haines R.F., Chuang S.L. The effects of video compression on acceptability of images for monitoring life sciences experiments1992. 45c. URL: ntrs.nasa.gov/search.jsp?R=19920024689.

РАЗРАБОТКА МЕТОДА КОНТРОЛЯ ЦЕЛОСТНОСТИ ИЗОБРАЖЕНИЯ НА ОСНОВЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

И.С. Чикликчи, А.А. Смагин, Л.В. Нечитайлова, Н.И. Кушниренко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail:infsec2011@gmail.com

Разработка средств и методов защиты информационной целостности документов, в частности цифровых изображений, остается традиционно актуальной задачей. Известность получили методы контроля целостности контента с использованием скрытых цифровых водяных знаков. Целостность здесь может гарантироваться путем хеширования файла. Хеш-суммы изображений могут храниться в отдельной защищенной базе данных. Для удобства работы системы желательно, чтобы хеш или другой модификатор, который гарантирует целостность, был встроен непосредственно в изображение. Подавляющее большинство цифровых фотографий хранится в сжатом виде с использованием алгоритмов группы JPEG. Поскольку алгоритм не хранит точные значения пикселей, добавление цифрового водяного знака (ЦВЗ) в файлы такого типа предусматривает добавление информации в пространстве преобразований, то есть, изменении подлежат квантованные коэффициенты дискретного косинусного преобразования (ДКП), именно те данные, которые остаются неизменными в процессе сжатия изображение. В качестве ЦВЗ выступать хеш-сумма изображения, получаемого путем использования хэш-функции. В алгоритмах, работающих с изображением такого формата, обычно меняются младшие значащие биты (LSB), и информация внедряется последовательно. В данной статье разработан метод контроля целостности изображения на основе цифрового водяного знака, который базируется на встраивании хеш-суммы в менее заметные места изображения и позволяет оценить психовизуальную заметность внедрения. На этапе перед встраиванием проводится анализ статистики изображения с целью выявления наиболее удачных мест для встраивания дополнительной информации. Приведенные результаты вычислительного эксперимента.

Ключевые слова: контроль целостности изображений, дискретное косинусное преобразование, цифровой водяной знак, встраивание секретной информации, хеш-сумма.

DEVELOPMENT OF A METHOD FOR IMAGE INTEGRITY CONTROL BASEDON DIGITAL WATERMARK

I.S. Chiklikchi, A.A. Smagin, L.V. Nechitailova, N.I. Kushnirenko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: infsec2011@gmail.com

The development of tools and methods to protect the information integrity of documents, in particular digital images, remains a traditionally important task. Methods for controlling the integrity of content using hidden digital watermarks have become popular. Integrity here can be guaranteed by hashing the file. Image hashes can be stored in a separate secure database. For the convenience of the system, it is desirable that the hash or other modifier that guarantees integrity, was embedded directly in the image. The vast majority of digital photos are stored in compressed form using JPEG group algorithms. Because the algorithm does not store exact pixel values, adding a digital watermark (DWC) to files of this type involves adding information in the transformation space, in other words, quantized discrete cosine transform coefficients (DCTs) are subject to change, namely those data that remain unchanged during compression. image. The hash sum of the image obtained by using the hash function will act as the CEV. Algorithms that work with an image of this format usually change the least significant bits (LSB), and the information is implemented sequentially. This article develops a method of image integrity control based on a digital watermark, which is based on embedding a hash sum in the least visible places of the image and allows you to assess the psycho-visual visibility of the implementation. At the stage before embedding, the analysis of image statistics is performed in order to identify the most successful places for embedding additional information. The results of a computational experiment are given.

Keywords: image integrity control, discrete cosine transformation, digital watermark, embedding of secret information, hash sum.