Предлагаемые изменения направлены на улучшение распределенной модели использования ресурсов и уменьшение вероятности угрозы конфиденциальности, целостности и доступности данных, другими словами, становится возможным снижение риска несанкционированного использования ресурсов.

Список литературы

1. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.
2. Townsend Stephen. Managing Risk: It’s Not Just for Big Business, IS 8930 Information Security Administration, Summer 2010,7/14/2010.
3. Beachboard John. Issues in Informing Science and Information Technology Volume 5, 2008. Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda. John Beachboard, Alma Cole, Mike Mellor, Steven Hernandez, Kregg Aytes, Idaho State University, Pocatello, Idaho USA; Nelson Massad, Florida Atlantic University, Florida USA.
4. Software Engineering Institute Carnegie Mellon [Электронный ресурс] // Режим доступа: http://www.cert.org/octave/.
5. Stoianov Nikolai Todorov , Tselkov Veselin Tsenov. E-net models for distribution, access and use of resources in security information systems [Электронный ресурс] // Режим доступа: http://arxiv.org/abs/1011.3148.

УДК 004.056

О.Ю. Головатюк
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення реалізації прихованих цифрових водяних знаків з використанням методів псевдоголографії

Все більшого значення в нашому світі, що швидко змінюється, набуває захист інформації. Давно існують два напрямки рішення цієї задачі: криптографія та стеганографія. Метою криптографії є приховування змісту повідомлень за допомогою їх шифрування. На відміну від цього, стеганографія приховує сам факт існування таємного повідомлення.

В даний час популярність досліджень в області стеганографії викликана двома причинами: обмеження на використання засобів криптографії в низці країн світу і поява проблеми захисту прав власності на інформацію, представлену в цифровому вигляді. Перша причина спричиняє за собою велику кількість досліджень приховання факту передачі інформації, друга – численні роботи в області цифрових водяних знаків [1].

Цифровий водяний знак (ЦВЗ) – спеціальна мітка, що непомітно вбудовується в зображення або іншу цифрову інформацію з метою контролювати її використання.

Метою даної роботи є розробка програмного забезпечення для приховування цифрових водяних знаків у зображеннях, використовуючи методи псевдоголографії.

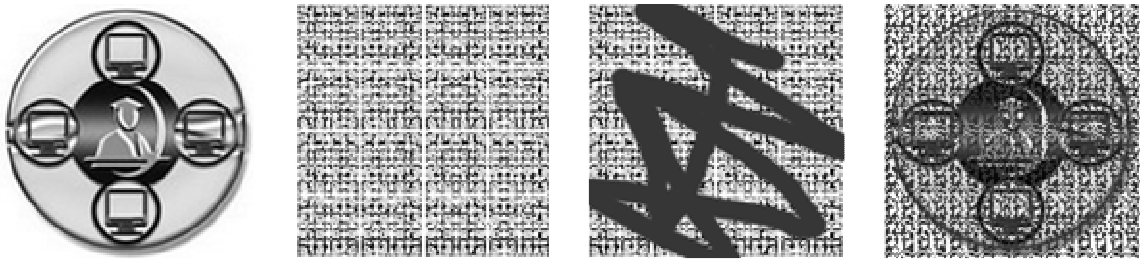
Найважливіша властивість голографії полягає в тому, що якщо відламати шматочок голограми, то в ньому буде видно ціле зображення [2]. Застосування голографії для приховуваних цифрових водяних знаків у вигляді зображень надає можливість відновлення ЦВЗ меншої роздільної здатності з будь-якого шматочка їх

голограми. Також можливе відновлення контурів початкового ЦВЗ, якщо відсутня чи пошкоджена значна частина його голограми. Тобто стає можливим вилучення ЦВЗ з пошкодженого чи видозміненого зображення та встановлення його справжнього автора (чи власника).

Біт-реверсивна перестановка має вищенаведені голографічні властивості [3].

Суть методу полягає в наступному. Припустимо, є послідовність довжиною 2^L. Кожен елемент цієї послідовності має індекс від 0 до 2^{L-1}. У двійковому представленні індекс буде виглядати $(b_{L-1}b_{L-2}\ldots b_1b_0)_2$. Тоді реверс бітів цього індексу буде виглядати $(b_0b_1\ldots b_{L-2}b_{L-1})_2$. Наприклад, дана послідовність символів A, B, C, D, E, F, G, H. Індексами цієї послідовності є числа: 0, 1, 2, 3, 4, 5, 6, 7; або в двійковому вигляді: 0b000, 0b001, 0b010, 0b011, 0b100, 0b101, 0b110, 0b111. Спочатку потрібно переставити біти кожного числа у зворотному порядку з урахуванням максимальної довжини двійкового числа (L = 3): 0b000, 0b100, 0b010, 0b110, 0b001, 0b101, 0b011, 0b111 (десяткові числа: 0, 4, 2, 6, 1, 5, 3, 7.) Потім елементи вихідної послідовності переставляються відповідно отриманим індексам: A, E, C, G, B, F, D, H. Таким чином, вийшла перестановка послідовності в біт-реверсному порядку. Суміжні пари AE, CG, BF, DH складаються з елементів, які розташовані в різних половинках вихідної послідовності. Щоб перетворити двомірне зображення, достатньо переставити біти в обох координатах кожного пікселя.

На рисунку 1а показаний цифровий водяний знак, на рисунку 1б його псевдоголограма. Квадратам кожних чотирьох пікселів голограми відповідає один піксель кожної чверті початкового зображення в досить хаотичному порядку. Із цього можна зробити висновок, що при біт-реверсивній перестановці пікселів зображення, великі елементи зображення стають дрібними, а дрібні великими.



а) *б)* *в)* *г)*

Рисунок 1 – відновлення пошкодженої псевдоголограми: а – ЦВЗ, б – його голограма, в – пошкоджена голограма, г – відновлений ЦВЗ із пошкодженої голограми

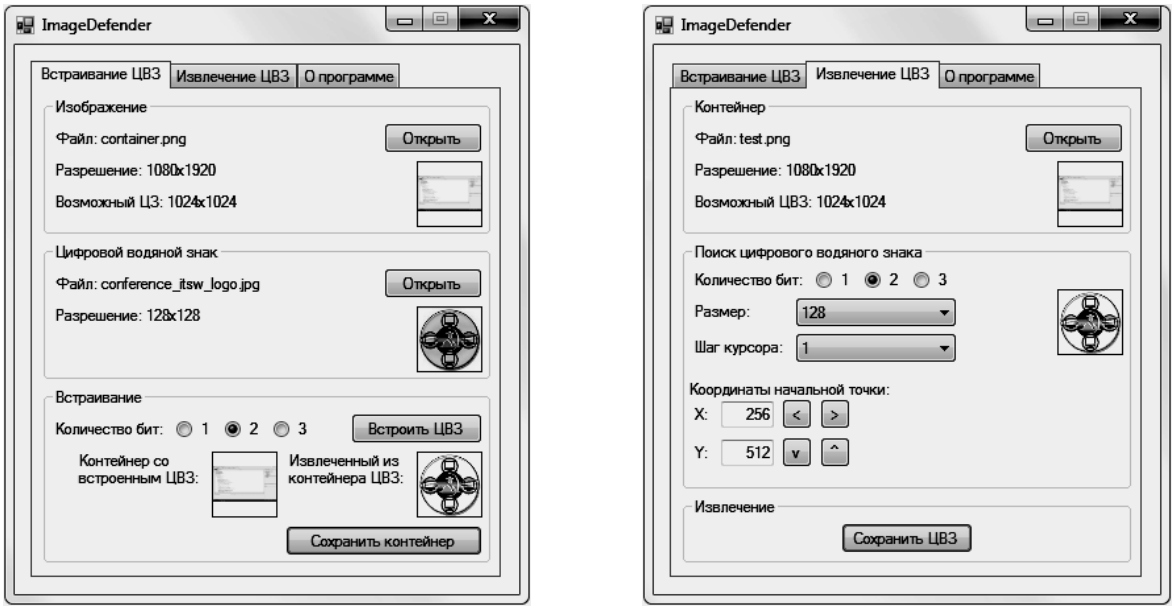
На рисунку 1 (в) показана голограма ЦВЗ з нанесеним низькочастотним шумом. Після відновлення початкового зображення, низькочастотний шум перетворився на високочастотний, однаково розподілений по всьому зображенню, але не зіпсував його пізнаваність.

Важливо, що біт-реверсивна перестановка може бути застосована тільки для послідовностей довжиною рівною степені двійки (4, 8, 16 і так далі). Також, при відновленні частини зображення воно повинно мати роздільну здатність рівну степені двійки і починатися з кратної їй позиції.

Псевдоголограму цифрового водяного знаку можна приховати в контейнер за допомогою одного з методів стеганографії – LSB методу (Least Significant Bit, найменший значущий біт).

Суть цього методу полягає в заміні останніх значущих бітів у контейнері на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини [1].

В розробленій програмі реалізовано отримання псевдоголограми графічного ЦВЗ за допомогою біт-реверсивної перестановки пікселів та її приховування у зображенні з глибиною кольору 24 біти на піксель за допомогою методу LSB.



а) *б)*

Рисунок 2 – інтерфейс програми: а – вбудовування ЦВЗ, б – вилучення ЦВЗ

Програма має інтуїтивно зрозумілий інтерфейс, показаний на рисунку 2, та проста у користуванні. Щоб сховати у зображенні цифровий водяний знак, потрібно відкрити контейнер, ЦВЗ та обрати кількість молодших біт (від 1 до 3), куди він буде прихований. Якщо роздільна здатність ЦВЗ не рівна степені двійки, виводиться пропозиція привести її до 2^N або використати його центральну частину. При натисненні на зменшені зображення, відкривається вікно для перегляду їх в оригінальному розмірі з можливістю зміни масштабу. При вбудовуванні ЦВЗ, він заміщується по всій площі зображення. Для вилучення цифрового водяного знаку потрібно відкрити зображення, обрати кількість задіяних молодших біт, вказати його розмір та початкові точки.

Основними результатами, отриманими у ході виконання даної науково-практичної роботи є:

– Досліджені та обґрунтовані переваги використання методів псевдоголографії в алгоритмах вбудовування прихованих цифрових водяних знаків.

– Реалізовано алгоритм, що створює псевдоголограму цифрового зображення за допомогою біт-реверсної перестановки пікселів зображення.

– Реалізовано алгоритм вбудовування прихованого цифрового знаку у графічні файли LSB методом.

– Розроблено програмне забезпечення на мові програмування C#, що здійснює вбудовування у графічні файли прихованих цифрових водяних знаків з використанням методів псевдоголографії.

Список літератури

1. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М.: Солон-Пресс, 2009 – 272 с.
2. Голография – Википедия [Електронний ресурс] // Режим доступу: http://ru.wikipedia.org/wiki/Голография.
3. Голографические свойства бит-реверсивной перестановки [Електронний ресурс] / Сергей Шишминцев // Режим доступу: http://habrahabr.ru/post/155471.