УДК 004.056.5

Г. А. Дмитрук
В. В. Карпінець

ВДОСКОНАЛЕННЯ СТЕГАОГРАФІЧНОГО МЕТОДУ PVD ДЛЯ ЗАХИСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Вінницький національний технічний університет

Анотація

Проаналізовано стеганографічні методи захисту цифрових зображень. Обрано для вдосконалення стеганографічний метод PVD. У вдосконаленому методі використано модифіковану ТКД, для точного вираховування місця вбудовування та витягування ЦВЗ, а також запропоновано використовувати мінімальне значення різниці пікселів у двох або в трьох напрямках.

Ключові слова: цифрова стеганографія, цифрові водяні знаки, контейнер, вбудоване (приховане) повідомлення, таблиця діапазонів квантування.

.

Abstract

Steganographic methods of digital image protection are analyzed. The steganographic PVD method was chosen for improvement. In the advanced method, a modified TRQ is used to accurately calculate the place of embedding and extraction of the CEV, and it is proposed to use the minimum value of the pixel difference in two or three directions.

Keywords: digital steganography, digital watermarks, container, built-in (hidden) message, table of quantization ranges.

Авторське право є інструментом власності, права і ключовою галуззю права інтелектуальної власності; воно призначене захищати зовнішню форму вираження об'єкта (твір, малюнок, збірник, фотографія та інше), тобто їхнє «матеріальне втілення». Авторське право не може використовуватись для захисту абстрактних ідей, концепцій, фактів, стилів та технік, що можуть бути використані у творі [1].

Актуальність проблеми визначається тим, що, більша половина всіх авторських творів, які ми можемо вільно знайти в мережі Інтернет, знаходяться саме з порушенням прав інтелектуальної власності. Численним є і недобросовісне ставлення до знаків, доменних імен. Крім того ЗМІ часто використовують з мережі фото та іншу інформацію на шпальтах своїх видань видаючи пізніше за знімки власних кореспондентів. І якщо авторство на друкований твір ще можна довести, то з величезним інформаційним простором – Інтернет ситуація значно гірша [2].

ЦВЗ можуть містити деякий автентичний код, тобто закодовану інформацію про власника або інформацію управління. Найбільш відповідними об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, як правило, логотипи [3].

На відміну від друкарського водяного знаку, який є чим-небудь видимим (наприклад, логотип), цифровий водяний знак створюється так, щоб бути невидимим, або у випадку з аудіо кліпами – нечутним. Більш того, біти, що представляють водяний знак, повинні бути розкидані усередині файлу так, щоб вони не могли бути ідентифіковані або змінені. Цифровий водяний знак повинен бути стійким, щоб витримувати такі зміни файлу, як масштабування, обертання, компресія з втратами (lossy compression) і інші. Невидимі ЦВЗ аналізуються спеціальним де-кодером, який покликаний виносити ухвалу про їх валідність [4].

Для вирішення проблем спотворень пропонуються різні техніки, але такі викривлення діяли чуйно у галузях військової, медичної та художньої роботи. Як результат, оборотні методи приховування даних активно досліджуються не лише для відновлення вихідного зображення обкладинки, але й для отримання секретних даних [5,6]. LSB (Найменший значущий біт) і PVD (Піксельна різниця) - типові приклади методів приховування даних. LSB - це техніка приховування секретних даних у найменш значущі біти, щоб людське око не могло легко їх розпізнати [3]. Як правило, коли секретні дані приховуються за допомогою до 3 найменших значущих бітів, спотворення зображення не може сприйматися людськими очима. Однак спотворення зображення може сприйматися людськими очима, коли найменш значущі біти використовуються більше 4. Для подолання проблеми спотворення запропоновано оптимальний алгоритм заміни LSB [7], і Wang et al. запропонував вдосконалену схему з використанням генетичного алгоритму [8].

Технологія PVD визначає розмір секретних даних, які можна приховати, використовуючи значення різниці двох послідовних пікселів у блоці. На зображеннях є гладка область і область краю. Крайова область порівняно складніше, ніж гладка. Коли зображення спотворене, зміну гладкої

області в людському оці можна добре розрізнити, але зміна області краю погано розрізнити. Отже, ми можемо приховати більше секретних даних в області краю, ніж у гладкій області, приховуючи секретні дані на зображенні.

У цій роботі пропонується нова схема стеганографії з використанням PVD різноспрямованості на кольорових зображеннях для вбудовування ЦВЗ [8]. Ми ділимо кольорове зображення на блоки, що не перекриваються, і розкладаємо кольорові пікселі в кожному блоці на R, G та B. Розкладені пікселі виконують перегрупування та знаходять мінімальне значення для застосування схеми PVD у двох напрямках або трьох напрямках. Пари пікселів, на яких була виконана схема PVD з модифікованою таблицею діапазонів квантування, зберігаються у двох зображеннях і генерують два стегозображення [9].

У таблиці 1 порівнюється показник якості запропонованої схеми та схеми Шива та Арупа . Індекс якості запропонованої схеми подібний до схеми Шива та Арупа.

Таблиця 1 Порівняння значень індексу якості вбудованого ЦВЗ модифікованими методами

Назва картинки	Схема Шива і Арупа Індекс якості	Запропонована схема			
		У двох напрямках		У трьох напрямках	
		Індекс якості – 1	Індекс якості – 2	Індекс якості – 1	Індекс якості – 2
Лена	0.6870	0.7653	0.7325	0.7735	0.7148
Тіфані	0.4686	0.4181	0.4563	0.3767	0.4863
Папуги	0.4486	0.4456	0.4401	0.4477	0.4348
Пляж	0.3297	0.3346	0.3284	0.3451	0.3190
Ручки	0.2370	0.2248	0.2354	0.2221	0.2362
Дівчнка	0.0712	0.0719	0.0693	0.0733	0.0677
Кіт	0.3792	0.3804	0.3755	0.3802	0.3756
Квітка	0.3294	0.3415	0.3344	0.3456	0.3300
Середнє зн.	0.3688	0.3727	0.3714	0.3705	0.3705

У таблиці 2 наведено експериментальні результати для кожного випадку, коли секретні дані вбудовуються у два напрямки та три напрямки в запропоновану схему.

Таблиця 2. Результати параметрів PSNR та ємномності вбудованого ЦВЗ представленим методам

Назва зображення	Запропонований метод					
	Два напрямки			Три напрямки		
	PSNR-1 (дБ)	PSNR-2 (дБ)	Ємність (біт)	PSNR-1 (дБ)	PSNR-2 (дБ)	Ємність (біт)
Лена	30.9791	32.2565	3,739,287	26.9258	29.5024	5,671,307
Тіфані	30.2070	30.4749	3,678,830	27.6425	30.8193	5,557,627
Папуги	30.5083	32.7829	3,643,723	28.0548	30.2345	5,507,035
Пляж	35.1747	36.2268	3,597,199	32.1241	35.2979	5,420,140
Ручки	29.8021	32.4704	3,643,788	28.2435	30.0250	5,563,465
Дівчнка	30.2782	32.9632	3,670,028	28.7210	30.4778	5,601,851
Кіт	34.0405	36.0262	3,591,096	33.2151	35.9475	5,429,264
Квітка	30.3256	32.8820	3,621,236	29.1141	31.1358	5,494,673
Середнє зн.	31.4144	33.2603	3,648,148	29.2551	31.6800	5,530,670

Отже, в даній роботі було розглянуто захист авторського права на цифрове зображення та детально проаналізовано стеганографічний метод приховування ЦВЗ в цифрових зображеннях PVD. Також було розроблено алгоритм вдосконалення стеганографічного методу PVD. Запропоновано використати модифіковану таблицю діапазонів квантування для вбудовування інформації в цифрове зображення. Також запропонована схема приховування даних із використанням різноспрямованої різниці значень пікселів на основі кольорового зображення. Експериментальні результати продемонстрували, що запропонована схема має високу здатність до вбудовування та прийнятну непомітність у якості візуального зображення.

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. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

3. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2013. – 152 с.

4. Карпінець В. В. Аналіз впливу цифрових водяних знаків на якість векторних зображень / В. В. Карпінець, Ю. Є. Яремчук // Сучасний захист інформації. — 2011. — № 1. — С. 72—82.

5. Стеганография в XXI веке. Цели. Практическое применение. Актуальность//Хабрахабр. Дата оновлення: 15.03.2015. [Електронний ресурс]. Режим доступу: https://habrahabr.ru/post/253045/.

6. Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=330&lvl

7. Стеганография [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki.

8. Стеганография, цифровые водяные знаки и стеганоанализ: [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. —М.: Вузовская книга, 2009. —220

9. Khalid,A. Darabkh. A New Steganographic Algorithm Based on Multi Directional PVD and Modifed LSB / Khalid A. Darabkh, Ahlam K. Al-Dhamari, and Iyad F. Jafar // Journal of Information Technology and Control. —2017. —Vol. 46, No. 1.

Дмитрук Ганна Анатоліївна — студентка групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: anytka2227@ukr.net

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

Dmitruk Hanna A. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, email : anytka2227@ukr.net

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