УДК 004.832

Телефус Д. В.
Лукічов В. В.

СТЕГАНОГРАФІЧНИЙ МЕТОД НА ОСНОВІ АЛГОРИТМУ HOG ТА МЕТОДІВ PVD-LSB

Вінницький національний технічний університет

Анотація
Розроблено адаптивний метод, що забезпечує вбудовування секретної інформації в цифрове зображення.
Ключові слова: стеганографія; прихована передача інформації; гістограма орієнтованого градієнта.
Abstract
An adaptive method for secret information embedding into digital images is developed.
Keywords: steganography; hidden information transmission; histogram of oriented gradient.

Вступ

Інформація є однією з найцінніших речей сучасного життя. Отримання доступу до неї з появою глобальних комп'ютерних мереж стало надзвичайно простим. Але легкість і швидкість такого доступу зробили значними й загрози безпеці даних за відсутності заходів щодо їх захисту, зокрема – загрози несанкціонованого доступу до інформації. Таким чинов виникає необхідність в забезпеченні захисту інформації, яка передається через незахищені канали зв'язку[1].

Стеганографія передбачає вбудовування секретного повідомлення у стеганографічний контейнер (наприклад, цифрове зображення) так, щоб не порушувати стійкість візуального сприйняття контейнера. Одною з основних вимог стеганографічного методу є його стійкість до різноманітних видів атак.

Сучасні стеганографічні методи дозволяють не лише приховано передавати дані (класичне завдання стеганографії – прихована передача даних (ППД)), але також успішно вирішувати завдання захисту інформації від несанкціонованого копіювання, завадостійкої автентифікації, відслідковування поширення даних мережами зв'язку, пошуку інформації в мультимедійних базах даних (БД).

Розробка методу

Різниця між значеннями пікселів (PVD) і найменш значущий біт (LSB) – широко поширені методи цифрової стеганографії. Ці два методи не враховують вміст зображення для приховування секретного повідомлення. Вміст більшості цифрових зображень має різні крайові напрями в кожному пікселі, і зовнішній вигляд локального об'єкта в основному характеризується розподілом його градієнтів інтенсивності або крайових напрямів. Використання цих характеристик для вбудовування секретної інформації в різні крайові напрями усуває необхідність послідовного вбудовування та покращує надійність. Тому пропонується застосувати алгоритм гістограми орієнтованого градієнта (HOG) для визначення напряму домінуючого краю для кожного блоку 2×2 зображення. Після цього використовується алгоритми PVD та LSB[2].

Запропонований метод адаптивної стеганографії складається з двох алгоритмів, один для вбудовування секретного повідомлення, а інший для його відновлення. Алгоритм вбудовування заснований на виборі набору блоків інтересу (BOI) з використанням алгоритму HOG. Розрахунок HOG вважається ключовим кроком запропонованого методу, при якому величина градієнта і кут обчислюються з горизонтального і вертикального градієнта зображення. Тоді кут градієнта обирається таким чином, щоб всі кути потрапляли в зазначений фіксований діапазон (1, 2, 3, 4, 5), що допомагає обробляти невеликі кутові відхилення. Щоб знайти напрям домінуючого краю для кожного блоку, гістограма орієнтованого градієнта розраховується для блоків розміром 2×2 пікселів. Для кожного BOI секретні дані вбудовуються в напрямку домінуючого краю із використанням алгоритму PVD і підстановка LSB для вбудовування інші двох пікселів. Граничне значення розраховується адаптивно відповідно

до довжини секретного повідомлення. На рисунку 1 зображено схему вбудовування секретного повідомлення.

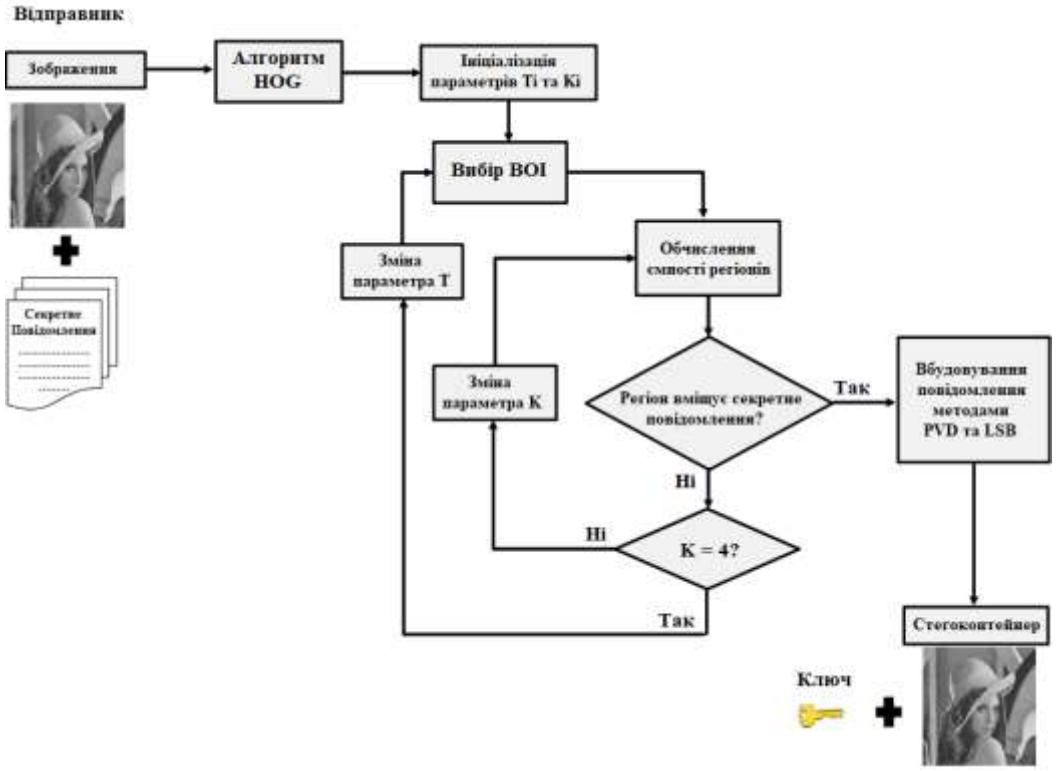

Рисунок 1 – Схема вбудовування секретного повідомлення запропонованим методом

Гістограма орієнтованого градієнта використовувався для вирішення проблеми виявлення об'єкта шляхом опису локальної інформації про краях об'єктів. Значення величини градієнта для кожного пікселя зберігається в залежності від відповідного йому кута. Потім, щоб знайти домінуючий кут θd для кожного блоку зображення обирається кут нахилу, який відповідає максимальному накопиченому значення величини градієнта *Gd*. Схему вбудовування секретного повідомлення зображено на рисунку 2.

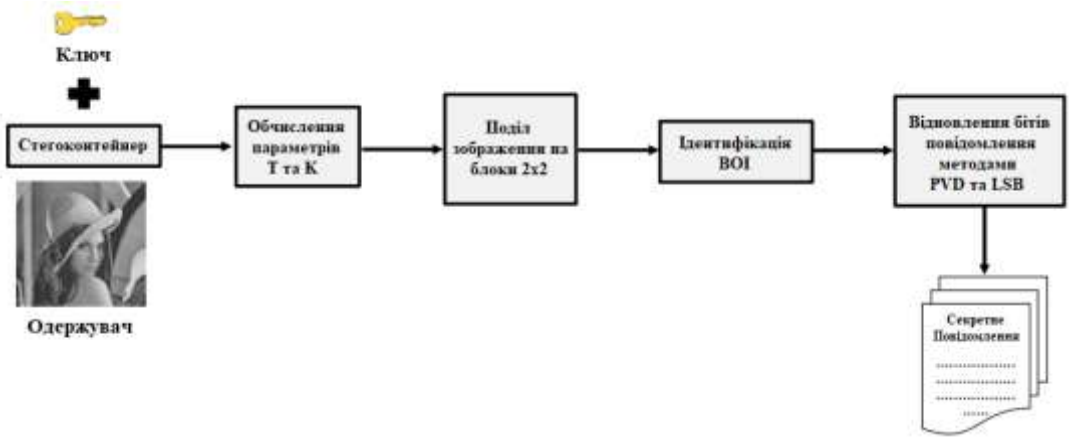

Рисунок 2 – Схема відновлення секретного повідомлення запропонованим методом

Блок інтересу – блок, який має значення величини градієнта більше обраного порогового параметра (T)[4]. Щоб знайти блок інтересу, значення величини домінуючого градієнта для кожного блоку обчислює ться шляхом знаходження максимального значення гістограми градієнта і пов'язаного з ним кута градієнта. Щоб уникнути блоків, що містять слабку крайову інформацію, максимальна

величина градієнта обмежується значенням *T*. Це значення адаптивно коригується на основі розміру секретного повідомлення. Граничне значення *T* знаходиться між 0 і 1. Нехай кількість крайових пікселів, що повертаються HOG детектор краю після порога дорівнює *N*. Цілком можливо що кількість крайових пікселів *K* може бути менше або більше ніж необхідний номер для конкретного секретного повідомлення *M*. Граничні значення *T* і *K* поступово збільшуються так, що повертає загальна кількість пікселів *K*, яке може поглинути все вбудовані біти.

Висновки

Аналіз відомих стеганографічних методів показав, що найбільш розповсюдженими методами приховування інформації в цифрових зображеннях є методи PVD та LSB.

Було розроблено метод адаптивного приховування даних з використанням гістограми орієнтованого градієнта (HOG) для вбудовування секретних даних в цифрові зображення на основі PVD-LSB

Розроблений метод підвищує рівень захисту інформації, що передається через незахищені канали зв'язку. Поєднання методів PVD-LSB і алгоритму HOG покращує пропускну здатність, візуальну якість і безпеку традиційних методів PVD і LSB.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. M. Hussain, A. W. A. Wahab, N. Javed, and K.-H. Jung, "Recursive information hiding scheme through LSB, PVD shift, and MPE," IETE Technical Review, vol. 35, no. 1, pp. 53–63, 2018.
3. N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in IEEE Computer Vision and Pattern Recognition (CVPR), vol. 1. IEEE, 2005, pp. 886–893.
4. J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," Signal Processing: Image Communication, vol. 29, no. 3, pp. 375–384, 2014.

Телефус Дмитро Володимирович — студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dmytro.telefus@gmail.com

Лукічов Віталій Володимирович — кандидат технічних наук, старший викладач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua

Telefus Dmytro V.— Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: dmytro.telefus@gmail.com

Lukichov Vitaliy V. — Candidate of Technical Sciences, Senior Lecturer of the Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua