004.056.55

В.О. Опанащук

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПРИХОВУВАННЯ ДАНИХ У ЦИФРОВИХ ЗОБРАЖЕННЯХ

Вінницький національний технічний університет

Анотація

У роботі досліджено напрямок підвищення ефективності приховування даних у цифрових зображеннях на основі стеганографічного методу PVD. Запропоновано вдосконалення класичного підходу шляхом використання колірної моделі YCbCr для зменшення візуальних спотворень, оператора Собеля для аналізу структури зображення та криптографічного алгоритму AES для додаткового захисту прихованої інформації. Запропонований підхід спрямований на підвищення непомітності вбудовування та захищеності переданої інформації.

Ключові слова: *стеганографія, приховування даних, PVD, YCbCr, оператор Собеля, AES, цифрові зображення.*

Abstract

The paper investigates approaches to improving the efficiency of data hiding in digital images based on the Pixel Value Differencing (PVD) steganographic method. An enhancement of the classical approach is proposed through the use of the YCbCr color model to reduce visual distortions, the Sobel operator for image structure analysis, and the AES cryptographic algorithm to provide additional protection of hidden information. The proposed approach is aimed at increasing the imperceptibility of data embedding and improving the security of transmitted information.

Keywords: *steganography, data hiding, PVD, YCbCr, Sobel operator, AES, digital images.*

Вступ

В умовах стрімкого розвитку інформаційних технологій цифрова стеганографія є важливим напрямом захисту інформації, що забезпечує приховування факту передачі даних шляхом їх вбудовування у цифрові контейнери, зокрема зображення, аудіо- та відеофайли. На відміну від криптографії, яка захищає зміст повідомлення, стеганографія приховує сам факт його існування.

Актуальність застосування стеганографічних методів зумовлена широким використанням відкритих каналів зв'язку та зростанням потреби у захисті конфіденційної інформації. Такі методи знаходять застосування у задачах прихованої передачі даних, захисту авторських прав, реалізації цифрових водяних знаків та організації захищених каналів комунікації [1].

Сучасний розвиток технологій штучного інтелекту сприяв появі ефективних методів стегоаналізу, здатних виявляти приховану інформацію за статистичними та структурними особливостями цифрових зображень. Проте одночасно відбувається вдосконалення стеганографічних підходів, спрямованих на підвищення непомітності вбудовування та стійкості до сучасних методів аналізу [2].

Таким чином, цифрова стеганографія залишається актуальним напрямом досліджень у сфері інформаційної безпеки, що зумовлює необхідність розробки та вдосконалення ефективних методів приховування інформації у цифрових зображеннях.

Метою роботи є вдосконалення підходу до приховування даних у зображеннях на основі стеганографічного методу PVD з використанням колірної моделі YCbCr, оператора Собеля та криптографічного алгоритму AES. На основі вдосконаленого підходу передбачається його подальша практична реалізація.

Результати дослідження

Метод різниць значень пікселів (PVD, Pixel Value Differencing) [3] належить до просторових методів цифрової стеганографії та базується на аналізі різниці яскравостей між сусідніми пікселями зображення.

Його принцип полягає в адаптивному визначенні обсягу даних, які можуть бути вбудовані в різні області контейнера. У ділянках із суттєвими змінами яскравості, таких як контури та текстурні області, можливо приховувати більшу кількість інформації без помітного впливу на візуальну якість зображення.

Натомість у гладких областях, де різниця між сусідніми пікселями є незначною, обсяг вбудованих даних обмежується для збереження непомітності змін.

Позначимо вхідне зображення у вигляді матриці пікселів:

$$I = \{p_1, p_2, \dots, p_N\},$$

де p_i – значення інтенсивності і-го пікселя, N – загальна кількість пікселів у зображенні.

Далі зображення розбивається на неперекривні пари сусідніх пікселів:

$$(p_i, p_{i+1}),$$

де p_iта p_{i+1} – значення яскравості двох сусідніх пікселів.

На етапі обчислення різниці для кожної пари визначається абсолютна різниця значень:

$$d = |p_i - p_{i+1}|,$$

де: d – різниця між значеннями пікселів, що характеризує локальну неоднорідність області зображення.

Множина можливих значень різниці d розбивається на інтервали:

$$R_k = [l_k, u_k],$$

де: R_k – k-й інтервал різниць; l_k – нижня межа інтервалу; u_k – верхня межа інтервалу.

Кількість бітів, які можна вбудувати в дану пару пікселів, визначається за формулою:

$$n = [log_2(u_k - l_k + 1)],$$

де: n – кількість бітів, що вбудовуються; $(u_k - l_k + 1)$ – кількість значень у відповідному інтервалі.

Для кодування повідомлення із потоку прихованого повідомлення вибирається n бітів, які інтерпретуються як десяткове число:

$$b \in [0, 2^n - 1],$$

де: b – числове представлення фрагмента повідомлення довжиною n бітів.

Для формування нової різниці нове значення різниці визначається як:

$$d' = l_k + b,$$

де: d' – модифікована різниця між пікселями, що містить закодовану інформацію.

Для модифікації пікселів необхідно змінити значення пікселів p_i та p_{i+1} таким чином, щоб нова різниця дорівнювала d'. Зміна значень виконується таким чином, щоб мінімізувати спотворення.

Загалом метод PVD забезпечує достатньо високу місткість контейнера за збереження прийнятної якості зображення, що робить його придатним для практичного застосування. Водночас, попри свої переваги, цей метод має певні обмеження, які можуть впливати на непомітність вбудовування та стійкість до виявлення прихованої інформації. Тому доцільним є його подальше вдосконалення шляхом усунення наявних недоліків. Основні недоліки методу та запропоновані підходи до їх усунення наведено в табл. 1.

Таблиця 1 – Підвищення захищеності приховування даних у цифрових зображеннях

Проблема	**Можливі шляхи вирішення**	**Запропоноване вдосконалення**	**Очікуваний результат**
Нерівномірність вбудовування інформації	Адаптивне вбудовування, використання додаткових характеристик зображення	Використання колірної моделі YCbCr [4] з розділенням на канали Y, Cb, Cr	Більш рівномірний розподіл вбудованих даних, підвищення ефективності використання контейнера
Ігнорування особливостей зорового сприйняття	Урахування моделі людського зору, обмеження змін у чутливих областях	Вбудовування переважно в канали Cb та Cr, мінімізація змін у каналі Y	Зменшення візуальних спотворень, підвищення непомітності
Вразливість до статистичного стегоаналізу	Адаптивний вибір областей, випадковість, комбінування методів	Використання оператора Собеля для аналізу структури зображення	Сприяє підвищенню стійкості до стегоаналізу

Продовження таблиці 1

Недостатня адаптивність до локальної структури зображення	Аналіз текстур, градієнтів, контексту	Використання градієнта (оператор Собеля) для регулювання параметрів PVD	Оптимальне вбудовування: мінімальні зміни в гладких областях і більше даних у текстурних
Відсутність захисту змісту повідомлення	Попереднє шифрування даних	Використання алгоритму AES перед вбудовуванням	Забезпечення конфіденційності навіть у разі виявлення повідомлення

Таким чином, запропоновані напрямки вдосконалення спрямовані на підвищення непомітності, адаптивності та стійкості методу до стегоаналізу. Використання колірної моделі YCbCr, оператора Собеля та алгоритму AES дозволяє усунути окремі недоліки класичного методу PVD, підвищити якість сформованого контейнера та забезпечити додатковий рівень захисту прихованої інформації. Запропонований підхід поєднує стеганографічні та криптографічні засоби захисту, що дозволяє розглядати його як комплексне рішення для безпечної передачі конфіденційної інформації цифровими каналами зв'язку.

Висновки

В роботі досліджено напрямок передачі даних у цифрових зображеннях засобами стеганографії. З метою вивчення можливостей вдосконалення підходу проведено аналіз існуючих методів приховування інформації та обґрунтовано вибір методу PVD як основи для подальшої роботи.

Запропоновано вдосконалення класичного методу PVD, яке полягає у використанні колірної моделі YCbCr та попередньому шифруванні повідомлення алгоритмом AES. Застосування колірної моделі YCbCr дозволяє розділити яскравісну та кольорові компоненти зображення, що сприяє зменшенню візуальних спотворень під час вбудовування даних та підвищенню непомітності прихованої інформації. Використання алгоритму AES забезпечує додатковий рівень захисту даних у випадку виявлення факту прихованої передачі інформації.

В подальшому, на основі запропонованого підходу, планується розробка програмного модулю мовою програмування C#, який реалізує функції вбудовування та вилучення прихованих даних із цифрових зображень. Для оцінки ефективності розробленого рішення буде проведено тестування та аналіз якості сформованих контейнерів із використанням метрик [5], зокрема, MSE та PSNR.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Increasing the efficiency of the steganographic system through the use of image processing methods. Modern Information Security. 2025. Т. 63, № 3. С. 68–74. URL: https://doi.org/10.31673/2409-7292.2025.030871 (дата звернення: 10.05.2026).

2. Khomiak R. M., Melnyk V. A. Implementation and comparative analysis of text steganography methods. Informatics. Culture. Technology. 2025. Т. 2. С. 71–80. URL: https://doi.org/10.15276/ict.02.2025.10 (дата звернення: 10.05.2026).

3. Image Steganography Using Pixel Value Differencing (PVD) Technique Based on Firefly Algorithm / O. M. Alade et al. Journal of Scientific Research and Reports. 2021. P. 80–86. URL: https://doi.org/10.9734/jsrr/2021/v27i730414 (дата звернення: 10.05.2026).

4. Alwan Z. A., Farhan H. M., Mahdi S. Q. Color image steganography in YCbCr space. International Journal of Electrical and Computer Engineering (IJECE). 2020. Т. 10, № 1. С. 202. URL: https://doi.org/10.11591/ijece.v10i1.pp202-209 (дата звернення: 10.05.2026).

5. Ткаченко В. П. Використання віртуальних метрик для оцінки якості кольорових зображень / В. П. Ткаченко, А. С. Гордєєв // Поліграфія і видавнича справа. 2023. 1(85). С. 65-72.

Опанашук Віктор Олегович – студент групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця

Науковий керівник: ***Зоря Ірина Сергіївна*** − асистент кафедри Менеджменту та безпеки інформаційних систем, e-mail: ira.zoria@vntu.edu.ua

Opanashchuk Viktor O. – student of group 1CITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Zoria Iryna S.*** − assistant of the Department of Management and Security of Information Systems, e-mail: ira.zoria@vntu.edu.ua