№ 5(59)
2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.93:004.056.55

https://doi.org/10.52058/2786-6025-2026-5(59)-6034-6048

**Супрун Ольга Миколаївна** кандидат фізико-математичних наук, доцент, доцент кафедри теорії та технології програмування, Київський національний університет імені Тараса Шевченка, м. Київ, ehttps://orcid.org/0000-0002-1196-5655

**Дудник Олександр Олександрович** кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0000-0003-0375-2606

**Кісєль Анатолій Георгійович** кандидат технічних наук, старший науковий співробітник, доцент кафедри комп'ютеризованих систем та програмних технологій, Інститут комп'ютерних систем, Національний університет «Одеська політехніка», м. Одеса, https://orcid.org/0000-0002-9760-0445

# СЕГМЕНТАЦІЯ ЗОБРАЖЕНЬ ЧЕРЕЗ КОМП'ЮТЕРНИЙ ЗІР ДЛЯ ІДЕНТИФІКАЦІЇ ОПТИМАЛЬНИХ ЗОН ПРИХОВУВАННЯ ДАНИХ

**Анотація.** У статті здійснено огляд сучасних підходів до цифрової стеганографії та можливостей їхнього поєднання з алгоритмами сегментації зображень для підвищення ефективності приховування інформації.

Акцентовано на застосуванні методів комп'ютерного зору та глибокого навчання для визначення оптимальних ділянок цифрових зображень, придатних для вбудовування стеганографічних повідомлень. Проаналізовано ефективність класичних алгоритмів, зокрема інтеграцію у найменш значущий біт, та сучасних моделей, що ґрунтуються на нейронних мережах, генеративних підходах і семантичному аналізі.

Наголошено на поєднанні сегментаційних підходів із сучасними методами стеганографії для підвищення непомітності вбудованих повідомлень, покращення якості зображень за показниками пікового відношення сигналу/шуму, індексом структурної подібності та підвищення стійкості до методів стеганоаналізу. Підкреслено, що традиційні методи обмежені відсутністю адаптації до локальних текстурних та семантичних характеристик зображень, що знижує рівень непомітності прихованих даних. Розкрито потенціал використання сегментаційних алгоритмів для ефективнішого визначення областей, придатних для приховування інформації, та обґрунтовано доцільність

ISSN 2786-6025 Online

застосування глибоких нейронних мереж, генеративних моделей і адаптивних механізмів вибору сегментів. Показано, що така інтеграція сприяє покращенню показників якості зображень за метриками показника пікового відношення сигналу/шуму та індексу структурної подібності, підвищує непомітність прихованих повідомлень та стійкість систем до сучасних методів стегано-аналізу. Доведено, що використання семантичного аналізу та адаптивного розподілу даних між сегментами зображення забезпечує вищу ефективність і надійність стеганографічних систем. Обґрунтовано перспективність поєднання методів комп'ютерного зору, сегментації та сучасних алгоритмів стеганографії для створення стійких і непомітних систем приховування інформації.

**Ключові слова:** цифрова стеганографія, сегментація зображень, комп'ютерний зір, глибоке навчання, стеганоаналіз.

**Suprun Olha Mykolaivna** Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Programming Theory and Technology, Taras Shevchenko National University of Kyiv, Kyiv, https://orcid.org/0000-0002-1196-5655

**Dudnyk Oleksandr Oleksandrovych** Candidate of Technical Sciences, Associate Professor of the Department of Software, Vinnytsia National Technical University, Vinnytsia, https://orcid.org/0000-0003-0375-2606

**Kisiel Anatolii Heorhiiovych** Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department of Computerized Systems and Software Technologies, Institute of Computer Systems, Odesa Polytechnic National University, Odesa, https://orcid.org/0000-0002-9760-0445

## IMAGE SEGMENTATION THROUGH COMPUTER VISION FOR IDENTIFYING OPTIMAL DATA HIDING ZONES

**Abstract.** The article provides a review of contemporary approaches to digital steganography and explores the potential for integrating them with image segmentation algorithms to enhance information-hiding efficiency. Special emphasis is placed on applying computer vision and deep learning methods to identify optimal regions in digital images for embedding steganographic messages. The effectiveness of classical algorithms, such as least-significant-bit embedding, as well as modern models based on neural networks, generative approaches, and semantic analysis, is analyzed.

Particular attention is given to combining segmentation-based approaches with advanced steganography methods to improve the imperceptibility of embedded

ISSN 2786-6025 Online
messages, enhance image quality (peak signal-to-noise ratio and structural similarity index), and increase resilience to steganalysis techniques. It is emphasised that traditional methods are limited by their lack of adaptation to the local textural and semantic characteristics of images, thereby reducing the imperceptibility of hidden data. The potential of segmentation algorithms for more effectively identifying regions suitable for information hiding is revealed, and the rationale for employing deep neural networks, generative models, and adaptive segment selection mechanisms is justified. It is demonstrated that such integration contributes to improved image quality metrics in terms of peak signal-to-noise ratio and structural similarity index, enhances the imperceptibility of hidden messages, and strengthens the system's resistance to modern steganalysis methods. The use of semantic analysis and adaptive distribution of data across image segments is shown to provide higher efficiency and reliability for steganographic systems. The study concludes that combining computer vision, segmentation, and modern steganography algorithms holds promise for developing robust and imperceptible information-hiding systems.
**Keywords**: digital steganography, image segmentation, computer vision, deep learning, steganalysis.

**Постановка проблеми.** За сучасних умов захист інформації у цифровому середовищі виходить далеко за межі класичної криптографії. Стеганографія як мистецтво прихованого передавання даних усередині медіаконтейнерів, є дедалі актуальнішим інструментом там, де факт існування секретного повідомлення не повинен бути розкритий. Проте між теоретичною ідеєю непомітного вбудовування і її практичною реалізацією існує суттєвий розрив, зумовлений передусім відсутністю обґрунтованого підходу до вибору зон зображення, придатних для розміщення прихованих даних. Найпоширеніші методи просторового вбудовування, зокрема метод найменш значущого біту (LSB), діють за принципом рівномірного або псевдовипадкового розподілу змін по всій площині зображення. Це окреслює дві взаємопов’язані вразливості. По-перше, модифікації неминуче потрапляють у семантично виразні або візуально однорідні ділянки: фони, гладкі поверхні, обличчя, де навіть мінімальні зміни яскравості статистично аномальні й легко виявляються. По-друге, рівномірне внесення шуму руйнує природну структуру просторових кореляцій між пікселями, залишаючи відбиток, доступний для сучасних алгоритмів стеганоаналізу.

Розв’язання цього завдання полягає не лише в удосконаленні механізму вбудовування, а й у переосмисленні логіки вибору місця для нього. Зображення є неоднорідним середовищем: деякі його ділянки насичені текстурою, шумом, складними перепадами яскравості, інші – монотонні й прозорі для будь-якого аналізу. Перші природно поглинають і маскують артефакти модифікації, а

ISSN 2786-6025 Online

другі, навпаки, їх підкреслюють. З огляду на це розв'язання завдання інтелектуальної ідентифікації зон, придатних для вбудовування, є принципово важливим для стеганографічної системи.

Комп'ютерний зір, зокрема методи сегментації зображень, надають для цього необхідний інструментарій. Сегментація дає змогу автоматично виокремлювати семантично та текстурно однорідні регіони, класифікувати їх за ступенем складності та визначати ті ділянки, де вбудовування залишатиметься непомітним як для людського сприйняття, так і для статистичного аналізу. Поєднання такого попереднього аналізу структури зображення із процедурою стеганографічного кодування формує принципово новий, інтегрований підхід до побудови прихованого каналу передавання даних.

Отже, актуальною науково-практичною проблемою є розроблення методу сегментації зображень засобами комп'ютерного зору, орієнтованого на ідентифікацію оптимальних зон для стеганографічного приховування даних. Розв'язання цієї проблеми безпосередньо впливає на два базові показники якості стеганографічної системи – непомітність вбудовування та стійкість до стеганоаналітичних атак – і є передумовою створення надійних засобів захисту прихованих комунікацій.

**Аналіз останніх досліджень і публікацій.** Наукові дослідження у сфері стеганографії зображень останніх п'яти років охоплюють широкий спектр підходів: від удосконалення класичних просторових методів до побудови складних архітектур глибинного навчання. Простеживши логіку їхнього розвитку, продемонстровано, як поступово змінювався фокус уваги дослідників, починаючи із пошуку шляхів вбудовування до визначення його місця.

Підґрунтям для цього процесу залишається метод LSB як базовий еталон просторового вбудовування. Так, його програмну реалізацію для приховування текстових даних у графічних файлах досліджують учений М. Б. Головін зі співавторами, показавши, що при коректній реалізації метод забезпечує прийнятний рівень непомітності шляхом мінімальних змін молодших бітів пікселів. Водночас вони зафіксували принципове обмеження підходу: відсутність вибірковості щодо зон вбудовування, що зумовило наступний етап [1]. Метод LSB розвивають автор Я. Я. Деміркан із колегами (Y. Y. Demircan et al.), інтегрувавши у нього попередню сегментацію зображення: вбудовування здійснювалося лише у текстурно складних зонах, що суттєво знизило статистичну помітність прихованого повідомлення та підвищило стійкість до виявлення [2]. Це дослідження уперше формалізувало ідею структурно обґрунтованого вибору місця вбудовування.

Одночасно розвивався напрям вибору самого зображення-контейнера. Зокрема, концепцію диверсифікованого вибору обкладинки, де критерієм слугує різноманіття текстурних характеристик потенційних контейнерів, що

ISSN 2786-6025 Online

дає змогу мінімізувати передбачуваність місць вбудовування, пропонують дослідник С. Лі зі співавторами (X. Li et al.) [3]. Розв'язання цієї проблеми з позиції стеганоаналізу пропонують науковець Х. Цао зі співавторами (H. Cao et al.), з'ясувавши, що навіть адаптивний вибір контейнера залишає помітні сліди без додаткових механізмів маскування змін [4]. Ці дослідження окреслили діалектику проблеми: вибір контейнера є необхідною, але недостатньою умовою безпеки системи.

Значний прорив у підвищенні непомітності вбудовування забезпечив перехід до частотних просторів. Метод стеганографії у просторі DCT із використанням глибинного навчання з підкріпленням, де агент самостійно навчався адаптивно розподіляти приховані дані між частотними коефіцієнтами залежно від їхньої чутливості до виявлення, розробляють автор Р. Янг із колегами (R. Yang et al.) [5]. Додатково, поєднання вейвлет-перетворення з генеративно-змагальними мережами (приховане повідомлення розміщувалося у субсмугах вейвлет-розкладання, де воно природно зливалося з коефіцієнтами деталізації зображення) досліджують учений Й. Яо зі співавторами (Y. Yao et al.) [6].

У цьому контексті наймасштабніші зміни у методології стеганографії пов'язані з упровадженням архітектур глибинного навчання. Двопотокову архітектуру на основі U-Net із направними крайовими картами вивчають дослідники П. Джі (P. Ji), Й. Чжанг (Y. Zhang) та З. Лв (Z. Lv), де мережа використовувала межі об'єктів як природні орієнтири для концентрації вбудовування у зонах із різкими перепадами яскравості, де артефакти є найменш помітними [7].

Метод на основі згорткових нейронних мереж з адаптивною функцією втрат, яка динамічно балансує між збереженням якості зображення та місткістю вбудовування, розробляють науковці П. Маласі (P. Malathi) та Т. Гіріш Кумар (T. Gireesh Kumar) [8]. А багаторівневу архітектуру, де послідовне кодування через кілька шарів суттєво підвищує стійкість повідомлення до стеганоаналітичних атак, показують автор Й. Саньялаве із колегами (Y. Sanjalawe et al.) [9].

Генеративні підходи розкрили ще один вимір задачі – семантичний, який спирається на спільне кодування змістової інформації кількох об'єктів зображення. Це завдання, де розподіл схованого вмісту узгоджувався зі смисловою структурою сцени, що робило вбудовування семантично мотивованим, розв'язують учені К. Ші (K. Shi), П. Ліу (P. Liu) та С. Лі (S. Li) [10]. Крім того, приховування у латентному просторі зображень з інтелектуальним вибором декодера – підхід, що дає змогу підтримувати якість реконструкції навіть за умов різнорідних спотворень, досліджують науковець Й. Чжоу зі співавторами (Y. Zhou et al.) [11].

ISSN 2786-6025 Online

Нарешті, необхідним складником будь-якої стеганографічної системи є надійна метрика якості. Тож, метод кількісного оцінювання візуальної якості цифрових кольорових зображень, що сприяє об'єктивній фіксації деградації контейнера після вбудовування, розробляють учені Ю. Журавель та Л. Мичуда. Вони дослідили роль фрактальних розмірностей як критерію вибору зон вбудовування, де показано, що ділянки із високою фрактальною складністю текстури природно поглинають стеганографічні модифікації, залишаючи їх непомітними [12; 13].

Таким чином, у дослідженнях розглянуто етапи від довільного вбудовування до структурно й семантично обґрунтованого вибору зон. Водночас питання поєднання автоматичної сегментації зображень засобами комп'ютерного зору із задачею ідентифікації оптимальних стеганографічних зон залишається нерозв'язаним, що й визначає напрям запропонованого дослідження.

**Мета статті** – дослідження можливостей використання алгоритмів сегментації зображень у системах комп'ютерного зору для визначення оптимальних зон приховування інформації у цифрових зображеннях та обґрунтування підходу, який поєднує методи сегментації зображень із сучасними алгоритмами стеганографії.

**Виклад основного матеріалу дослідження.** Інноваційні рішення у галузі цифрової стеганографії демонструють значний прогрес у розробленні методів приховування інформації у цифрових зображеннях. Проте більшість класичних методів, зокрема LSB вбудовування, обмежені через відсутність адаптації до локальних текстурних та семантичних особливостей зображень. Експериментальні дослідження на вибірках понад 500 зображень високої роздільної здатності показали, що традиційні методи LSB забезпечують показники PSNR у межах 36–38 дБ та SSIM 0,92–0,94, водночас стійкість до стандартних атак стеганоаналізу не перевищує 65 % [1, с. 83–85; 14]. Ці дані підкреслюють обмеження класичних алгоритмів у забезпеченні непомітності та надійності сучасних стеганографічних систем.

Методично такі показники отримують шляхом порівняння оригінального та зміненого зображень із використанням PSNR та SSIM. Для цього формується тестова вибірка зображень із різним рівнем текстурної складності, після чого здійснюється приховування повідомлень методом LSB. Далі обчислюються статистичні відхилення між вихідними та модифікованими зображеннями. Такий підхід широко застосовується у сучасних дослідженнях стеганографії для оцінювання непомітності та ефективності алгоритмів приховування даних [12, с. 40–42].

Крім того, стрімкий розвиток цифрових технологій, постійне зростання обсягів мультимедійних даних та активне поширення мережевих комунікацій створюють нові виклики у сфері захисту інформації. Це зумовлює потребу

ISSN 2786-6025 Online

удосконалювати методи приховування даних у цифрових зображеннях, роблячи їх ефективнішими та непомітнішими. Отже, дослідники дедалі частіше звертаються до інтелектуальних алгоритмів оброблення зображень, які здатні враховувати не лише технічні параметри, а й структурні та семантичні особливості візуального контенту.

Це сприяє підвищенню надійності систем приховування інформації та їхній стійкості до сучасних методів аналізу завдяки використанню алгоритмів комп'ютерного зору, що охоплюють попереднє оброблення зображень (нормалізацію яскравості, виділення контурів, аналіз текстурних характеристик і побудову карт складності) та сегментацію [15, с. 69–71]. Отримані параметри дають змогу визначати ділянки, де приховування інформації є найменш помітним, що підвищує ефективність стеганографічних операцій і загальну надійність системи.

Зокрема, використання Edge Guided Dual Stream U-Net на вибірці 1000 зображень ImageNet продемонструвало підвищення точності сегментації ділянок із різною текстурною складністю на 12 % порівняно з базовим U-Net, що забезпечує більш оптимальне розміщення прихованої інформації.

Відповідно, показник PSNR збільшився на 1,8 дБ, а SSIM – на 0,03, що засвідчує покращення візуальної якості [7].

Запропонована модель ґрунтується на двопотоковій архітектурі нейронної мережі, де один потік аналізує текстурні особливості зображення, а інший — контурні характеристики та межі об'єктів. Поєднання цих потоків забезпечує формування більш точних карт сегментації, які використовуються для вибору ділянок із високою текстурною складністю. Саме у таких зонах приховані зміни залишаються найменш помітними як для людського ока, так і для алгоритмів стеганоаналізу [7].

Зокрема, застосування сегментації зображень у стеганографії забезпечує гнучке та контекстно орієнтоване розміщення прихованих повідомлень. Завдяки алгоритмам комп'ютерного зору можна аналізувати текстурну складність, контрастність і семантичну структуру окремих ділянок зображення. Це зумовлює адаптивний вибір зон, у яких зміни залишаються практично непомітними як для людського ока, так і для автоматизованих систем аналізу. Такий метод дає змогу значно підвищити ефективність приховування даних, роблячи стеганографічні системи більш надійними та стійкими до сучасних методів виявлення.

Сегментація може здійснюватися різними способами: через кластеризацію пікселів, аналіз меж об'єктів, використання глибоких нейронних мереж або комбінованих алгоритмів. Отримані сегменти мають власні статистичні характеристики: дисперсію яскравості, ентропію текстури та локальну контрастність, які аналізують, наскільки вони придатні для приховування

ISSN 2786-6025 Online

інформації, і забезпечують більш точний вибір зон для стеганографічних операцій [2, с. 314–318].

У цьому процесі глибокі нейронні мережі з латентним просторовим вбудовуванням та адаптивним вибором декодера дають змогу істотно підвищити результативність стеганографічного приховування даних у цифрових зображеннях, зокрема покращення непомітності вбудованих повідомлень і збереження візуальної якості контейнера. На вибірці 1200 зображень така модель оптимально адаптує приховування даних до локальних контекстів, досягаючи PSNR ≈ 39,2 дБ і SSIM 0,97 при стійкості до атак 85–90 % [11]. Семантично підсилені підходи, що поєднують деформацію візуальних ознак із навчанням глибоких мереж, покращують непомітність повідомлень на 10–12 % і підвищують SSIM до 0,96 на вибірці 800 зображень [16].

У таких системах використовується латентний простір нейронної мережі, де інформація про зображення подається у вигляді багатовимірних ознак. Приховування повідомлень відбувається не безпосередньо у піксельній структурі, а у цих латентних демонстраціях. Це сприяє суттєвому зменшенню статистичних відхилень та майже непомітній трансформації змін, що підвищує рівень захищеності системи.

Водночас сучасні моделі глибокого навчання здатні не лише автоматично визначати оптимальні параметри для приховування інформації, а й гнучко підлаштовуватися під особливості конкретного зображення. Використання складних архітектур нейронних мереж гарантує детальний аналіз просторових та семантичних характеристик, що суттєво підвищує ефективність процесу вбудовування даних.

Застосування такого підходу забезпечує можливість розроблення більш надійних і малопомітних стеганографічних систем, що відповідають сучасним вимогам захисту інформації.

На цьому тлі генеративні моделі, які сприяють одночасному кодуванню багатьох об’єктів, підтверджують ефективність у сценаріях багатооб’єктного приховування: на вибірці 600 зображень PSNR зменшувався менше ніж на 0,5 дБ, а SSIM залишався ≥0,95 [10]. Це засвідчує, що генеративні підходи дають змогу адаптивно розподіляти приховану інформацію без втрати візуальної якості.

Методично генеративні моделі ґрунтуються на архітектурах генеративної змагальної мережі (GAN) або варіаційних автоенкодерах, які навчаються відтворювати структуру зображення. У процесі створення нових чи модифікованих зображень приховане повідомлення інтегрується безпосередньо в побудову піксельної структури [6]. Завдяки цьому воно є практично невіддільним від візуального контенту, що значно підвищує рівень непомітності та захисту.

ISSN 2786-6025 Online

Ще однією важливою перевагою генеративних моделей є їхня здатність створювати нові зображення або змінювати наявні так, щоб приховані повідомлення інтегрувалися у візуальну структуру максимально природно. Це забезпечує підвищення непомітності процесу приховування даних, що значно ускладнює їхнє виявлення та підвищує безпеку передавання інформації.

Стійкість до стеганоаналізу є надзвичайно важливою для стеганографічних методів, адже сучасні алгоритми аналізу зображень можуть досить точно виявляти навіть незначні статистичні зміни, які виникають під час вбудовування прихованої інформації. Так, адаптивні механізми уваги та DenseNet виявляють стандартні LSB-методи з точністю 92–94 % на вибірці понад 1000 зображень [4; 17, p. 1635–1638], що підкреслює необхідність поєднання сегментації та адаптивного вибору зон для підвищення безпеки стеганографічних систем.

Саме алгоритми стеганоаналізу здійснюють багаторівневий аналіз статистичних характеристик зображення: розподіл піксельних значень, кореляцію між сусідніми пікселями та особливості текстурної структури. Використання глибоких нейронних мереж дає змогу автоматично виявляти складні закономірності, які можуть показувати наявність прихованих даних [17, p. 1640–1643].

Таким чином, засвідчено, що розвиток методів стеганоаналізу відбувається паралельно з удосконаленням технологій приховування інформації. Отже, сучасні стеганографічні системи повинні ураховувати можливості інтелектуальних алгоритмів аналізу зображень, здатних виявляти навіть найменші статистичні відхилення у структурі цифрового контенту. Такий баланс між приховуванням і виявленням формує новий рівень вимог до безпеки та надійності систем передавання даних.

Згідно із цим особливого значення набуває оцінювання непомітності вбудовування даних, оскільки вона дає змогу кількісно проаналізувати, як саме стеганографічні методи впливають на структуру та візуальні характеристики зображення.

Кількісна експертиза непомітності демонструє, що ігнорування локальної складності сегментів погіршує PSNR і SSIM на 5–8 % [13, с. 76–78; 12, с. 41–43]. Використання фрактальних розмірностей дає змогу визначати сегменти з максимальною непомітністю для вбудовування даних. Застосування сегментації як окремого модуля забезпечує точне виділення семантичних сегментів і підвищує ефективність стеганографії на 10 % [2, p. 320–324]. Інші підходи, зокрема диференційований вибір контейнерів [3] або багаторівневі глибокі моделі [9], дійсно підвищують загальну надійність стеганографічних систем, але вони не забезпечують точне визначення локальних ділянок, де приховування інформації буде найефективнішим.

ISSN 2786-6025 Online

Метод фрактального аналізу передбачає обчислення фрактальної розмірності для різних ділянок зображення. Він гарантує оцінювання складності текстури та рівня хаотичності її структури. Зі зростанням фрактальної розмірності внесені зміни є менш помітними, що робить такі ділянки оптимальними для приховування інформації [13, с. 78–80].

Аналіз кількісних показників підкреслює важливість урахування локальних характеристик зображення під час вибору ділянок для приховування даних. Саме методи сегментації дають змогу поєднати статистичні, текстурні та семантичні параметри в єдиній моделі аналізу. Це забезпечує більш точне визначення оптимальних зон і сприяє підвищенню ефективності процесу приховування інформації, роблячи його стійкішим та менш помітним.

У практичних дослідженнях така інтеграція реалізується у вигляді модульних систем: блок сегментації виконує попередній аналіз зображення, а модуль стеганографії здійснює адаптивне приховування даних у визначених ділянках. Подібна архітектура підвищує ефективність процесу приховування та забезпечує гнучку адаптацію алгоритмів до різних типів зображень [18; 8].

У таблиці 1 наведено порівняльний аналіз класичних методів, зокрема LSB-вбудовування із сучасними підходами, що ґрунтуються на глибоких нейронних мережах, генеративних моделях та урахуванні семантичної інформації зображень, та їхнього потенціалу для інтеграції з алгоритмами сегментації. Наголошено на методах, які використовують сегментацію для визначення оптимальних зон приховування даних. Така практика дає змогу оцінити, як алгоритми враховують локальні текстурні та семантичні особливості зображень і як це впливає на непомітність та стійкість стеганографічної системи.

**Таблиця 1**

Огляд сучасних методів стеганографії з оцінюванням якості та стійкості до атак

| Метод | Вибірка (кількість зображень) | PSNR (дБ) | SSIM | Стійкість до атак (%) | Джерело |
|---|---|---|---|---|---|
| LSB-вбудовування | 500 (BOSSBase, USC-SIPI) | 36–38 | 0,92–0,94 | 60–65 | [1] |
| Edge Guided Dual Stream U-Net | 1000 (ImageNet) | 38–39,8 | 0,95–0,98 | 78–82 | [7] |
| Латентне просторове вбудовування зі Smart Decoder | 1200 | 39,2 | 0,97 | 85–90 | [11] |

ISSN 2786-6025 Online

| Метод | Вибірка (кількість зображень) | PSNR (дБ) | SSIM | Стійкість до атак (%) | Джерело |
|---|---|---|---|---|---|
| Семантично підсилена одночасна деформація ознак | 800 | 38,5 | 0,96 | 80–85 | [16] |
| Генеративне багатооб'єктне вбудовування | 600 | 39,0 | 0,95–0,96 | 82–88 | [10] |
| Адаптивний стеганоаналіз DenseNet | 1000 | N/A | N/A | 92–94 | [4; 5] |
| Сегментаційний LSB-підхід | 500–700 | 38,2 | 0,95 | 80 | [2] |
| Диференційований вибір контейнерів | 800 | 38,8 | 0,96 | 87 | [3] |
| Глибокий багаторівневий підхід | 900 | 39,1 | 0,97 | 88 | [9] |

Джерело: сформовано авторами

Таким чином, у таблиці 1 не лише узагальнено кількісні показники ефективності різних методів, але й закладено методологічне підґрунтя для подальших досліджень, підкреслюючи важливість поєднання сегментаційних алгоритмів комп'ютерного зору з адаптивними стеганографічними підходами для підвищення ефективності та надійності приховування інформації у цифрових зображеннях.

Отже, сучасні підходи – від глибокого навчання та генеративних моделей до семантично підсилених методів – показують, що основою до розвитку стеганографії є поєднання сегментації, комп'ютерного зору та адаптивних методів приховування даних. Така інтеграція не лише підвищує ефективність, непомітність і стійкість систем, а й відкриває перспективи для створення інтелектуальних рішень захисту інформації, здатних адаптивно обробляти візуальний контент і протистояти сучасним методам аналізу.

Отже, наукова цінність цього дослідження полягає у розробленні підходу, який поєднує алгоритми комп'ютерного зору для сегментації зображень із сучасними адаптивними методами приховування даних. Він дає змогу знаходити найефективніші локальні ділянки для вбудовування інформації, підвищувати якість прихованих зображень за показниками PSNR та SSIM, робити систему більш стійкою до новітніх атак стеганоаналізу, оцінювати непомітність і якість стеганоповідомлень у реальних умовах, де зображення мають складні текстури й семантику. У результаті його застосування

ISSN 2786-6025 Online

формується міцне методологічне підґрунтя для створення високоефективних і надійних стеганографічних систем, що є не лише теоретичною засадою, а й реальним інструментом сучасної кібербезпеки.

**Висновок.** Під час дослідження виявлено принципову закономірність: якість стеганографічної системи визначається до початку процесу вбудовування. Те, куди потрапляють приховані дані, виявляється важливішим за те, як саме вони кодуються. Доведено, що методи, які ураховують локальну текстурну складність, контурну структуру та семантику зображення, стабільно перевершують класичні підходи за усіма вимірюваними показниками: перехід від LSB до сегментаційно орієнтованих архітектур дає приріст PSNR на 1,2–3,2 дБ, виводить SSIM на рівень 0,97 і підіймає стійкість до атак із 60–65 % до 85–90 %.

У практичному вимірі висновок очевидний: блок сегментації засобами комп'ютерного зору має бути не факультативним доповненням, а обов'язковим першим модулем будь-якої сучасної стеганографічної системи. Виокремлення контурів, оцінювання фрактальної складності текстури, побудова карт семантичної структури – усе це формує точну карту зображення, де одні ділянки природно поглинають зміни, а інші їх демонструють. Ігнорувати цю карту означає свідомо залишати системі вразливості, якими сучасні алгоритми стеганоаналізу користуються із точністю до 92–94 %.

У довгостроковій перспективі дослідження окреслює напрям, у якому стеганографія уже не є суто технічною дисципліною, а перетворюється на інтелектуальну – читає зображення так само уважно, як це робить людське око.

Подальший розвиток цього напряму через поєднання сегментаційних алгоритмів із генеративними моделями та навчанням із підкріпленням здатний вивести системи прихованих комунікацій на рівень, де їхнє виявлення є практично нереальним.

Таким чином, майбутній розвиток галузі визначається синтезом комп'ютерного зору, штучного інтелекту та адаптивних стратегій приховування інформації, що формує науково обґрунтовану основу для підвищення надійності та ефективності цифрових стеганографічних систем.

***Література:***

1. Головін М. Б., Головіна Н. А., Гузачов Д. М. Програмна реалізація стеганографічного приховування текстової інформації в графічному файлі методом LSB. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2025. № 59. С. 82–87. DOI: https://doi.org/10.36910/6775-2524-0560-2025-59-11

2. Demircan Y. Y., Ozekes S. A Novel LSB steganography technique using image segmentation. *Journal of Universal Computer Science*. 2024. Vol. 30, № 3. P. 308–332. DOI: https://doi.org/10.3897/jucs.105702

ISSN 2786-6025 Online

3. Li X., Guo D., Qin C. Diversified cover selection for image steganography. *Symmetry*. 2023. Vol. 15, № 11. Article 2024. DOI: https://doi.org/10.3390/sym15112024

4. Cao H., Wang Z., Zhang X. On improving steganalysis against cover selection steganography. *Cybersecurity*. 2025. Vol. 8. Article 115. DOI: https://doi.org/10.1186/s42400-025-00423-z

5. Yang R., Liu L., Han B., Hu F. Deep reinforcement learning-based DCT image steganography. *Mathematics.* 2025. Vol. 13, № 19. Article 3150. DOI: https://doi.org/10.3390/math13193150

6. Yao Y., Wang J., Chang Q., Ren Y., Meng W. High invisibility image steganography with wavelet transform and generative adversarial network. *Expert Systems with Applications*. 2024. Vol. 249. Article 123540. DOI: https://doi.org/10.1016/j.eswa.2024.123540

7. Ji P., Zhang Y., Lv Z. Edge-guided dual-stream u-net for secure image steganography. *Applied Sciences*. 2025. Vol. 15, № 8. Article 4413. DOI: https://doi.org/10.3390/app15084413

8. Malathi P., Gireesh Kumar T. Deep steganographic approach for reliable data hiding using convolutional neural networks and adaptive loss optimization. *Scientific Reports*. 2025. Vol. 15. Article 45692. DOI: https://doi.org/10.1038/s41598-025-26867-4

9. Sanjalawe Y., Al-E'mari S., Fraihat S., Abualhaj M., Alzubi E. A deep learning-driven multi-layered steganographic approach for enhanced data security. *Scientific Reports*. 2025. Vol. 15. Article 4761. DOI: https://doi.org/10.1038/s41598-025-89189-5

10. Shi K., Liu P., Li S. A generative image steganography method based on joint encoding of multi-object semantic information. *Pattern Analysis and Applications*. 2025. Vol. 28. Article 201. DOI: https://doi.org/10.1007/s10044-025-01567-x

11. Zhou Y., Wang N., Hong X., Peng Y., Shao S. Deep learning-based image steganography with latent space embedding and smart decoder selection. *Entropy*. 2025. Vol. 27. № 12. Article 1223. DOI: https://doi.org/10.3390/e27121223

12. Журавель Ю. І., Мичуда Л. З. Метод кількісного оцінювання візуальної якості цифрових кольорових зображень. *Сучасний захист інформації*. 2024. № 4(60). С. 39–45. DOI: https://doi.org/10.31673/2409-7292.2024.040004

13. Журавель Ю. І., Мичуда Л. З. Методи підвищення непомітності та стійкості стеганоповідомлень із застосуванням фрактальних розмірностей. *Сучасний захист інформації*. 2025. № 1. С. 74–81. DOI: https://doi.org/10.31673/2409-7292.2025.011576

14. Kazmidi I., Zubok V. Image steganography – classic and promising methods: a study. *Theoretical and Applied Cybersecurity*. 2025. Vol. 7, № 1. P. 14–19. DOI: https://doi.org/10.20535/tacs.2664-29132025.1.328302

15. Журавель Ю. І., Онишко В. Р. Підвищення ефективності стеганографічної системи через застосування методів обробки зображень. *Сучасний захист інформації*. 2025. № 3. С. 68–74. DOI: https://doi.org/10.31673/2409-7292.2025.030871

16. Zhang F., Dong Y., Sun H. Research on key technologies of image steganography based on simultaneous deception of vision and deep learning models. *Applied Sciences*. 2024. Vol. 14, № 22. Article 10458. DOI: https://doi.org/10.3390/app142210458

17. He Z., Wu R., Wang X. Image steganalysis based on an adaptive attention mechanism and lightweight densenet. *Computers, Materials & Continua.* 2025. Vol. 85, № 1. С. 1631–1651. DOI: https://doi.org/10.32604/cmc.2025.067252

18. Liu B., Song W., Zheng M., Fu C., Chen J., Wang X. Semantically enhanced selective image encryption scheme with parallel computing. *Expert Systems with Applications*. 2025. Vol. 279. Article 127404. DOI: https://doi.org/10.1016/j.eswa.2025.127404

ISSN 2786-6025 Online

***References:***

1. Holovin, M. B., Holovina, N. A., & Huzachov, D. M. (2025). Prohramna realizatsiia stehanohrafichnoho pryhovuvannia tekstovoi informatsii v hrafichnomu faili metodom LSB [Software implementation of steganographic hiding of text information in a graphic file using LSB method]. *Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo – Computer-Integrated Technologies: Education, Science, Production*, (59), 82–87. https://doi.org/10.36910/6775-2524-0560-2025-59-11 [in Ukrainian].

2. Demircan, Y. Y., & Ozekes, S. (2024). A Novel LSB Steganography technique using image segmentation. *Journal of Universal Computer Science*, 30(3), 308–332. https://doi.org/10.3897/jucs.105702

3. Li, X., Guo, D., & Qin, C. (2023). Diversified cover selection for image steganography. *Symmetry*, 15(11), 2024. https://doi.org/10.3390/sym15112024

4. Cao, H., Wang, Z., & Zhang, X. (2025). On improving steganalysis against cover selection steganography. *Cybersecurity*, 8, 115. https://doi.org/10.1186/s42400-025-00423-z

5. Yang, R., Liu, L., Han, B., & Hu, F. (2025). Deep reinforcement learning-based DCT image steganography. *Mathematics*, 13(19), Article 3150. https://doi.org/10.3390/math13193150

6. Yao, Y., Wang, J., Chang, Q., Ren, Y., & Meng, W. (2024). High invisibility image steganography with wavelet transform and generative adversarial network. *Expert Systems with Applications*, 249, 123540. https://doi.org/10.1016/j.eswa.2024.123540

7. Ji, P., Zhang, Y., & Lv, Z. (2025). Edge-guided dual-stream u-net for secure image steganography. *Applied Sciences*, 15(8), 4413. https://doi.org/10.3390/app15084413

8. Malathi, P., & Gireesh Kumar, T. (2025). Deep steganographic approach for reliable data hiding using convolutional neural networks and adaptive loss optimization. *Scientific Reports*, 15, 45692. https://doi.org/10.1038/s41598-025-26867-4

9. Sanjalawe, Y., Al-E'mari, S., Fraihat, S., Abualhaj, M., & Alzubi, E. (2025). A deep learning-driven multi-layered steganographic approach for enhanced data security. *Scientific Reports*, 15, 4761. https://doi.org/10.1038/s41598-025-89189-5

10. Shi, K., Liu, P., & Li, S. (2025). A generative image steganography method based on joint encoding of multi-object semantic information. *Pattern Analysis and Applications*, 28, 201. https://doi.org/10.1007/s10044-025-01567-x

11. Zhou, Y., Wang, N., Hong, X., Peng, Y., & Shao, S. (2025). Deep learning-based image steganography with latent space embedding and smart decoder selection. *Entropy*, 27(12), 1223. https://doi.org/10.3390/e27121223

12. Zhuravel, Y. I., & Mychuda, L. Z. (2024). Metod kilkisnoho otsiniuvannia vizualnoi yakosti tsyfrovykh kolorovykh zobrazhen [Method for quantitative evaluation of visual quality of digital color images]. *Suchasnyi zakhyst informatsii – Modern Information Security*, (4(60)), 39–45. https://doi.org/10.31673/2409-7292.2024.040004 [in Ukrainian].

13. Zhuravel, Y. I., & Mychuda, L. Z. (2025). Metody pidvyshchennia nepomitnosti ta stiikosti stehanopovidomlen z zastosuvanniam fraktalnykh rozmirnostei [Methods to increase invisibility and robustness of steganographic messages using fractal dimensions]. *Suchasnyi zakhyst informatsii – Modern Information Security*, (1), 74–81.https://doi.org/10.31673/2409-7292.2025.011576 [in Ukrainian].

14. Kazmidi, I., & Zubok, V. (2025). Image steganography – classic and promising methods: a study. *Theoretical and Applied Cybersecurity*, 7(1), 14–19. https://doi.org/10.20535/tacs.2664-29132025.1.328302

15. Zhuravel, Y. I., & Onyshko, V. R. (2025). Pidvyshchennia efektyvnosti stehanohrafichnoi systemy cherez zastosuvannia metodiv obrobky zobrazhen [Enhancing

ISSN 2786-6025 Online
steganographic system efficiency through image processing methods]. *Suchasnyi zakhyst informatsii – Modern Information Security*, (3), 68–74. https://doi.org/10.31673/2409-7292 .2025.030871 [in Ukrainian].

16. Zhang, F., Dong, Y., & Sun, H. (2024). Research on key technologies of image steganography based on simultaneous deception of vision and deep learning models. *Applied Sciences*, 14(22), 10458. https://doi.org/10.3390/app142210458

17. He, Z., Wu, R., & Wang, X. (2025). Image steganalysis based on an adaptive attention mechanism and lightweight densenet. *Computers, Materials & Continua*, 85(1), 1631–1651. https://doi.org/10.32604/cmc.2025.067252

18. Liu, B., Song, W., Zheng, M., Fu, C., Chen, J., & Wang, X. (2025). Semantically enhanced selective image encryption scheme with parallel computing. *Expert Systems with Applications*, 279, 127404. https://doi.org/10.1016/j.eswa.2025.127404

*Дата першого надходження статті до видання: 28.04.2026*
*Дата прийняття статті до друку після рецензування: 13.05.2026*