

передаватися повторно багато разів, внаслідок чого на мережу лягає додаткове навантаження. Для оцінювання потенціальних характеристик безпроводової телекомунікаційної мережі з випадковим множинним доступом, змінними параметрами та структурою, працюючої в умовах зовнішніх завад, розроблено імітаційну модель мережі. З використанням розробленої моделі оцінені потенціальні характеристики мережі за умов зміни структури (числа термінальних вузлів, поступових та раптових змін характеристик мережного трафіку тощо).

Перелік посилань

1. Dordal P. An Introduction to Computer Networks - Release 1.9.18, 2019. 882p.
2. Vegesna S.R. IP Quality of Service. - Pearson Education, Cisco Press, 2019, 221 River Street, Hoboken, NJ 07030. 368 pp.
3. Recommendation E.800 : Definitions of terms related to quality of service Approved in 2008-09-23, Status : In force. Електронний ресурс. Режим доступу: <https://www.itu.int/rec/T-REC-E.800-200809-I>.
4. Ahmed Arshed Al-Shammari, Volodymyr Drovovozov, Oksana Ilkova, and Heorhii Krivykhovetskyi. Optimization and Analysis of Wireless Network Characteristics with Service Quality Maintaining. CMiGIN 2022: 2nd International Conference on Conflict Management in Global Information Networks, November 30, 2022, Kyiv, Ukraine.
5. Дрововозов В.І., Аль-Шаммарі Ахмед Аршед, Толстікова О.В. Оптимізація ключових характеристик безпроводових мереж з міжрівневою взаємодією. Проблеми інформатизації та управління: зб. наук. праць. К. НАУ, 2021. Вип. №67 (3). С. 16–27.
6. Дрововозов В. І., Аль-Шаммарі Ахмед Аршед, Толстікова О. В., Водоп'янов С. В., Коцюр А. Б. Наскрізна якість сервісу безпроводових мереж з міжрівневою взаємодією. Проблеми інформатизації та управління. 2020. Вип. 63. С. 11–17.
7. Khan M. A., Al-Fuqaha A. QoS-Aware Routing in 5G and Beyond Wireless Networks: A Survey // IEEE Communications Surveys & Tutorials. 2021. Vol. 23, no. 3. P. 1568–1617. DOI: 10.1109/COMST.2021.3074456 .
8. Wang Y., Chen X., Liu Z., Tao M. A Deep Reinforcement Learning Approach for QoS Routing in Dynamic Wireless Networks // IEEE Transactions on Network Science and Engineering. 2023. Vol. 10, no. 4. P. 2105–2119. DOI: 10.1109/TNSE.2023.3267891 .
9. Kumar S., Kumar R., Singh S. K. Energy-Efficient QoS Routing Protocol for Wireless Sensor Networks Using Multi-Objective Optimization // Sensors. 2020. Vol. 20, no. 15. Art. 4231. P. 1–25. DOI: 10.3390/s20154231 .
10. Li J., Shen H., Yang Y. Delay-Constrained Routing in Wireless Mesh Networks Using Lagrangian Relaxation // Computer Networks. 2022. Vol. 215. Art. 109123. P. 1–14. DOI: 10.1016/j.comnet.2022.109123 .
11. Zhang L., Wang K., Zhang N., Shen X. Self-Similar Traffic Modeling and QoS Provisioning in Next-Generation Wireless Networks // IEEE Access. 2021. Vol. 9. P. 72856–72870. DOI: 10.1109/ACCESS.2021.3078945 .
12. Al-Sayed M. A., El-Bakary H. M. F. A., Hassan A. A. A Tabu Search-Based QoS Routing Algorithm for IoT Networks // Ad Hoc Networks. 2024. Vol. 154. –Art. 103215. P. 1–12. DOI: 10.1016/j.adhoc.2024.103215 .
13. Duong T. Q., Nguyen H. H., Le-Ngoc T. Cross-Layer QoS Optimization in Wireless Multimedia Sensor Networks // Journal of Network and Computer Applications. 2020. Vol. 167. Art. 102721. P. 1–13. DOI: 10.1016/j.jnca.2020.102721 .

Надійшла 01.10.2025

УДК 004.056.55:004.93

DOI: 10.31673/2409-7292.2025.041208

Журавель Ю.І., Мичуда Л.З., Сколздра М.М.

ОЦІНЮВАННЯ ВПЛИВУ СЕМАНТИКИ ЗОБРАЖЕНЬ НА ЕФЕКТИВНІСТЬ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

У статті досліджено питання підвищення ефективності стеганографічних систем шляхом аналізу результатів приховування інформації при застосуванні різних алгоритмів вбудовування. Метою роботи є оцінювання впливу методу стеганографічного перетворення на візуальну непомітність контейнера та стійкість прихованих даних до деструктивних впливів. Проведено порівняння класичних алгоритмів LSB-модифікації з частотними методами на основі дискретного косинусного (DCT) та вейвлет-перетворення (DWT), а також з комбінованими підходами, що враховують просторово-частотну структуру зображення. Запропоновано комплекс критеріїв ефективності, який включає об'єктивні показники візуальної якості (PSNR, SSIM, MSE), нормовану середньоквадратичну похибку, а також показники стійкості до атак різного типу. У роботі наведено результати експериментальних досліджень ефективності стеганоалгоритмів із використанням наборів тестових зображень з різним семантичним наповненням. Показано, що структурно-змістові особливості зображення суттєво впливають на ефективність приховування: зображення зі складною текстурою забезпечують вищу ємність і візуальну

непомітність, тоді як гладкі однорідні області більш чутливі до внесених змін. Додатково оцінено стійкість прихованої інформації до дії атак JPEG-компресії, імпульсного шуму, фільтрації та геометричних трансформацій. Результати дослідження підтверджують, що підвищення ефективності стеганографічної системи можливе завдяки адаптивному вибору місця вбудовування, який враховує тип, семантику та статистичні характеристики зображення-контейнера. Отримані висновки можуть бути використані для розроблення нових інтелектуальних стеганосистем, що автоматично визначають оптимальні параметри вбудовування з метою досягнення балансу між візуальною непомітністю та стійкістю до атак.

Ключові слова: кіберзагрози, стеганографічний алгоритм, захист інформації, нейронні мережі, просторова та частотна область.

Вступ та формулювання проблеми

Відомо, що ефективність стеганографічних методів є комплексним поняттям. Вона залежить від багатьох факторів – алгоритму приховування, методів попередньої обробки стегоконтейнера, співвідношення об'ємів повідомлення та стегоконтейнера тощо. Суттєво на ефективність стеганографічних систем впливає семантичне наповнення зображень-стегоконтейнерів. Також серед основних складових слід виділити здатність прихованого повідомлення залишатися непоміченим для стороннього спостерігача, а також зберігати свою цілісність під впливом деструктивних факторів, що виникають у процесі передавання, зберігання або навмисних атак. Для чисельного аналізу цих складових здебільшого застосовують наступні критерії оцінки - візуальна непомітність, яка визначається відсутністю помітних артефактів у стегоконтейнері та стійкість до атак, тобто здатністю відновлювати вбудоване повідомлення після впливу спотворень різного характеру.

В цій роботі візуальну непомітність оцінювали за допомогою об'єктивних метричних показників, таких як пікове співвідношення сигнал/шум PSNR, індекс структурної подібності SSIM та нормалізована середньоквадратична помилка NRMSE, які дозволяють кількісно порівняти відмінності між оригінальним контейнером і стегозображенням. Стійкість до атак визначається шляхом аналізу здатності коректно відновити приховану інформацію після впливу шуму, JPEG-компресії, масштабування, фільтрації та інших типів обробки.

Метою цієї роботи є підвищення ефективності приховування інформації у цифрових зображеннях шляхом аналізу та порівняння різних алгоритмів вбудовування за критеріями візуальної непомітності, стійкості до атак та ємності контейнера, а також встановлення залежності ефективності стеганографічних методів від семантичних і структурних характеристик зображень.

Аналіз літератури

Семантика цифрового зображення визначається сукупністю візуальних об'єктів, їхньою структурною складністю, контекстом сцени та рівнем деталізації. На відміну від суто статистичних характеристик, які визначають розподіл інтенсивностей, спектральні коефіцієнти тощо, семантика відображає змістовну інформацію, яка сприймається людиною та алгоритмами комп'ютерного зору. Для випадку стеганографії цей фактор має критичне значення, оскільки саме зміст сцени впливає на маскування спотворень, виявлених при прихованні повідомлення. У ряді наукових праць [1, 2] зазначено, що ефективність стеганографічної системи (за критеріями ємності, стійкості та непомітності) варіюється залежно від семантичного типу зображення – наприклад, зображення з високою текстурною насиченістю (листя, шерсть, натовп) краще приховують артефакти, ніж зображення з великими однорідними ділянками (небо, стіни).

Проаналізуємо вплив семантичних особливостей на ключові характеристики стегосистеми.

Ємність (Capacity)

Ємність зображення до вбудовування прихованої інформації прямо залежить від локальної варіативності пікселів. Семантично насичені області (наприклад, рослинність, фактурні поверхні) мають значну кількість дрібних деталей, що дає можливість розподілити зміни амплітуди на малі ділянки без помітного впливу на якість.

Для кількісної оцінки використовується значення середньоквадратичного відхилення значень інтенсивностей в локальному околі:

$$C = \frac{1}{N} \sum_{i=1}^N \sigma_{local}(B_i), \quad (1)$$

де C – ємність; $\sigma_{local}(B_i)$ – локальне стандартне відхилення інтенсивностей в блоці B_i ; N – кількість блоків.

Окрім виразу (1) існують інші оцінки текстури локального околу. Це може бути ентропія, гістограмні оцінки, фрактальна розмірність [3] тощо. Усі вони також використовуються при побудові адаптивних методів приховування повідомлень.

Стійкість

Семантично важливі об'єкти з високим рівнем структурної надмірності краще зберігають приховану інформацію після спотворень (JPEG-компресія, шум, масштабування). Наприклад, приховане повідомлення в області "трави" має більше шансів на успішне відновлення після стискування, ніж у ділянці однорідного фону. Додавання невеликого рівня шуму на зображення також сприяє підвищенню ефективності стегосистеми [4].

Непомітність

Семантичне наповнення суттєво впливає на маскування артефактів. Візуально складні області здатні приховувати більші зміни без значного зниження візуальної якості, яка оцінюється параметром MOS. Дослідження [5, 6] показують, що при однаковій інтенсивності модифікацій сприйняття артефактів у текстурованих зонах є значно нижчою, ніж у гладких.

Як вже неодноразово зазначалося у численних наукових працях [4-6], у сучасних стеганографічних системах, орієнтованих на роботу з цифровими зображеннями, ключовим завданням є досягнення високої прихованої пропускну здатності за умови збереження візуальної непомітності модифікацій та стійкості до атак. Традиційно оптимізація алгоритмів зосереджувалася на використанні статистичних та перцептивних характеристик зображень, таких як енергія частотних компонентів, локальна варіація інтенсивності чи структурна складність. Проте з розвитком комп'ютерного зору та глибинного навчання стало можливим урахування семантичного наповнення зображення, тобто значення та важливості його окремих ділянок з точки зору людського сприйняття.

Підхід, що враховує семантику зображення, базується на тому, що зорове сприйняття людини нерівномірно чутливе до змін у різних областях сцени. Модифікації в текстурованих ділянках менш помітні, ніж у зонах, що містять ключові об'єкти або гладкі поверхні. Це відкриває можливість адаптивного розподілу вбудовуваної інформації – підвищення щільності приховування в семантично менш значущі області та зменшення інтенсивності модифікацій у критично важливих сегментах зображення.

Новітні методи врахування семантики у стеганографії ґрунтуються на сегментації сцен, визначенні областей інтересу, а також на використанні глибинних нейронних мереж для автоматичного аналізу об'єктів та контексту. Такий підхід дозволяє не лише зменшити ризик візуального виявлення, але й підвищити стійкість алгоритмів до статистичного аналізу, оскільки розподіл модифікацій стає більш природним та наближеним до властивостей оригінальної сцени.

Відповідно, дослідження методів, що враховують семантичну інформацію, є актуальним напрямом розвитку стеганографічних алгоритмів, особливо в умовах зростання можливостей автоматизованих систем виявлення прихованих повідомлень.

Таким чином, сучасний розвиток стеганографії демонструє зростаючу увагу до семантичного наповнення зображень, що визначає, які ділянки сцени є більш значущими для людського сприйняття та автоматизованого аналізу. Це дозволяє реалізувати адаптивні підходи до вибору областей вбудовування, підвищуючи непомітність та стійкість алгоритмів. На основі аналізу наукових робіт сформовано класифікацію стеганографічних методів, які враховують семантичне наповнення зображень (рис. 1).

У методах на основі сегментації та виділення областей інтересу стегосистема використовує алгоритми семантичної сегментації для поділу зображення на об'єкти та фон. Вбудовування здійснюється переважно у фонові або текстуровані області, де спотворення менш помітні [7].

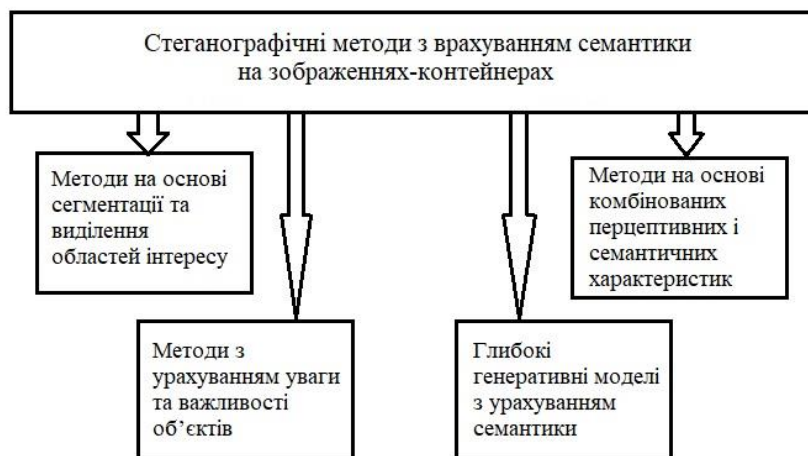


Рис. 1. Класифікація стеганографічних методів з врахуванням семантичного наповнення зображень-контейнерів

У методах з урахуванням уваги та важливості об'єктів використовуються механізми уваги, які дозволяють визначати релевантні для сприйняття зони зображення. Модифікації виконуються у малозначущих зонах, тоді як ключові об'єкти захищені від спотворень [8].

Використання глибоких генеративних моделей з урахуванням семантики та дифузійних моделей дозволяє створювати або модифікувати зображення з прихованою інформацією так, щоб вони залишалися семантично узгодженими. При цьому зміни інтегруються в структуру сцени, що робить їх майже непомітними [9].

Методи на основі комбінованих перцептивних і семантичних характеристик представляють собою поєднання традиційних моделей візуальної чутливості (наприклад, PSNR-HVS, SSIM) із семантичними картами та дозволяють досягти кращого компромісу між сміністю та непомітністю [10].

Отже, сучасні методи з врахуванням семантичного наповнення демонструють значно вищу якість прихованого передавання повідомлень, оскільки враховують не лише низькорівневі характеристики зображення, але й його змістовну структуру, що безпосередньо впливає на сприйняття людиною та складність виявлення. Семантичне наповнення є суттєвим фактором, що визначає ефективність стеганографічних методів.

Аналіз ефективності приховування інформації при застосуванні різних алгоритмів вбудовування

У цьому дослідженні виконано експериментальне оцінювання низки методів вбудовування інформації у просторовій області, зокрема:

- методу найменш значущого біта (НЗБ);
- методу псевдовипадкового інтервалу;
- методу псевдовипадкової перестановки;
- методу блокового приховування;
- методу заміни палітри;
- методу квантування зображення;
- методу Куттера–Джордана–Боссена.

За стегоконтейнер використано відоме тестове зображення Lena розміром 512×512 пікселів, у яке було вбудовано уривок поетичного твору Т. Г. Шевченка («Заповіт»).

Проведено порівняльний аналіз зазначених методів з точки зору досягнення оптимального балансу між непомітністю приховування та стійкістю до можливих атак, а також визначення найефективніших підходів для практичного застосування в системах захисту інформації (табл. 1).

Таблиця 1

Значення параметрів PSNR, SSIM та NRMSE для методів приховування у просторовій області

Метод	PSNR (дБ)	SSIM	NRMSE
НЗБ (LSB)	52,1	0,998	0,008
Псевдовипадковий інтервал	49,7	0,996	0,011
Псевдовипадкова перестановка	48,9	0,994	0,013
Блокове приховування	46,5	0,991	0,015
Заміна палітри	44,2	0,987	0,018
Квантування зображення	42,8	0,983	0,021
Куттера–Джордана–Боссена (CJB)	40,5	0,978	0,024

Природно, що результати роботи більшості методів суттєво залежать від умов експерименту та налаштувань. Для прикладу, у методі LSB може застосовуватися адаптивне вбудовування або просте. Тому для можливості порівняння у всіх методах за можливості приймали одні і ці ж налаштування – колірна модель, число колірних каналів, методи попередньої обробки, параметри стиску і т.п.

Значення параметрів у таблиці 1 слід інтерпретувати наступним чином: PSNR (dB) – чим більше, тим краща візуальна непомітність; SSIM – від 0 до 1, ближче до 1 – менше помітні спотворення; NRMSE – нормована середньоквадратична похибка, чим менше значення, тим краще. Метод вбудовування у найменш значущий біт демонструє найвищі значення PSNR і SSIM. Це свідчить про майже непомітне візуально вбудовування, але потенційно менш стійке до атак (наприклад, JPEG-компресії). Методи псевдовипадкового інтервалу і псевдовипадкової перестановки дещо знижують візуальну якість, але підвищують стійкість за рахунок розподілу даних по зображенню. Значення параметрів ефективності, які обчислені для методів блокового приховування та заміни палітри є компромісом між непомітністю та стійкістю. Метод квантування зображення та CJB мають нижчі значення PSNR і SSIM, оскільки змінюють більше пікселів, але забезпечують вищу стійкість до деяких методів обробки зображення.

Експериментальні дослідження ефективності стеганоалгоритмів з використанням наборів зображень з різним семантичним наповненням

Проведено експериментальне дослідження значень основних параметрів ефективності для зображень-стегоконтейнерів з різним семантичним наповненням. Для цього було вибрано три кольорові зображення з відомої бази тестових зображень [11] (рис. 2).



а)



б)



в)

Рис. 2. Тестові зображення.

Зображення на рисунку 2 відрізняються семантичним наповненням. На основі кожного з них сформовано ще 24 зображення з різними типами (шум, розмиття, стиск) та рівнями (від

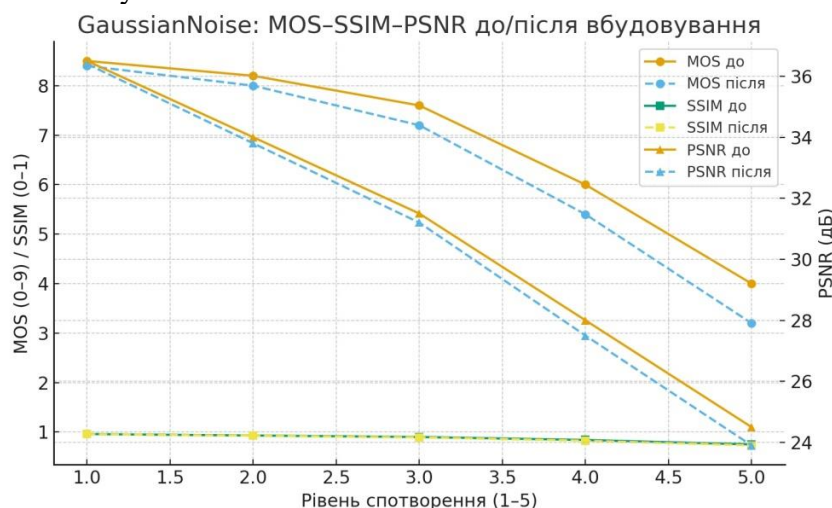
1 до 5) спотворень. Кожному зображенню з спотвореннями відповідає числова експертна оцінка, що робить цю базу прийнятною для тестування нових алгоритмів.

Методика експерименту буда наступною. У набори з різними типами і коефіцієнтом спотворень, які були сформовані на основі зображень на рис. 2, вбудовувалося повідомлення – «Заповіт» Тараса Шевченка методом адаптивного LSB. Далі проводилися обчислення наступних параметрів – пікове співвідношення сигнал/шум PSNR, оцінка структурної подібності SSIM, нормалізована середньоквадратична похибка NRMSE та експертна оцінка візуальної якості заповненого стегоконтейнера MOS.

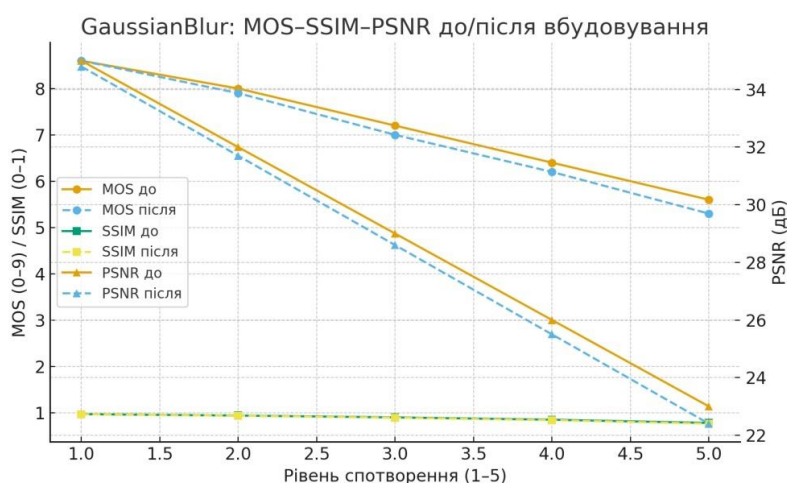
Проведемо аналіз отриманих результатів. Для зручності аналізу числові результати експерименту представлені у вигляді графіків (рис. 3).

Кількісна оцінка візуальної якості **MOS (Mean Opinion Score)** має достатньо високий рівень кореляції як із значеннями пікового співвідношення сигнал/шум **PSNR**, так і з індексом структурної подібності **SSIM** до і після вбудовування повідомлення. Після вбудовування значення PSNR і SSIM дещо знижуються, але характер залежності з MOS зберігається – тобто суб'єктивна оцінка якості (MOS) змінюється прогнозовано. Найбільше падіння якості спостерігається для високих рівнів спотворення (4–5) при накладанні гаусівського шуму (GaussianNoise) та JPEG, тоді як гаусовське розмиття (GaussianBlur) дає більш «м'яке» зниження MOS, навіть при зменшенні PSNR.

Проаналізуємо зміну значень оцінки візуальної якості MOS за типами спотворень – шуму, розмиття та стиску.



а)



б)

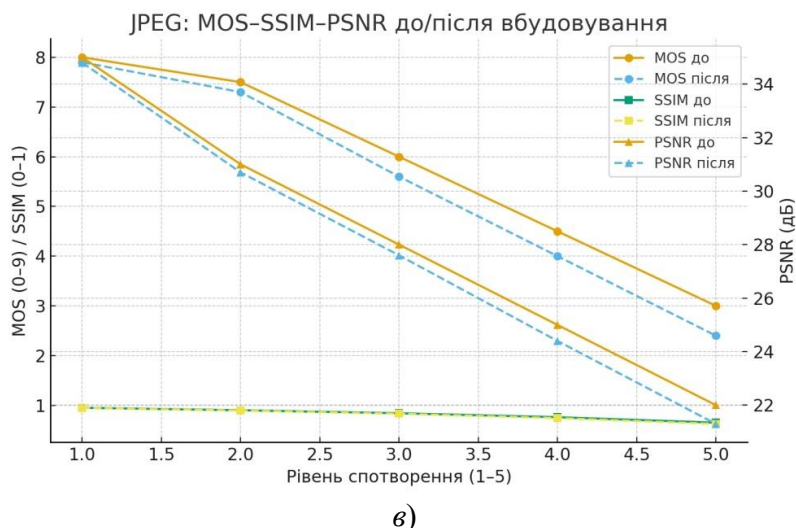


Рис. 3. Графіки залежностей параметрів оцінки візуальної якості MOS, PSNR і SSIM при дії різних типів спотворень – шуму (а), розмиття (б) і стиску (в) - до та після вбудовування.

При низьких рівнях шуму (рис. 3а) MOS падає повільно, а при високих – різко. Вбудовування інформації підсилює деградацію на рівнях 4–5, що помітно і по PSNR, і по SSIM. Семантика зображення спотворюється найбільше на дрібних деталях і текстурі – вони «зливаються» з шумом.

У випадку розмиття (рис. 3б) MOS знижується більш лінійно, навіть при падінні PSNR. Вбудовування практично не впливає на візуальне сприйняття семантичних об'єктів (контури лишаються читабельними). Тут суб'єктивна якість більше залежить від чіткості контурів, ніж від абсолютного рівня шуму.

Вплив стиску (рис. 3в) представляє особливий інтерес для задач стеганографії. Зміна MOS і PSNR відбувається ступінчасто. Різке падіння спостерігається на низьких рівнях якості JPEG. Після вбудовування артефакти блоків стають дещо більш помітними, особливо в областях з високою текстурною складністю. Для зображень з важливими дрібними деталями (текст, дрібні об'єкти) ефект на семантику критичний.

Проаналізуємо вплив спотворень з точки зору семантичного наповнення стегоконтейнера. До вбудовування зображення з чіткими об'єктами та великими однорідними ділянками зберігають семантику навіть при PSNR ~28–30 дБ, але при дрібній текстурі деградація помітна раніше. Після вбудовування спостерігається зменшення PSNR і SSIM, яке не завжди пропорційне втраті семантики. Наприклад, GaussianBlur може давати помірно низький PSNR, але об'єкти лишаються впізнаваними. Найкритичніший фактор для збереження семантики – поєднання сильного шуму та втрати високочастотних компонент (JPEG на низькій якості + GaussianNoise). Загалом PSNR та SSIM зберігають майже лінійну залежність з MOS, навіть після вбудовування. Лінії тренду для GaussianNoise та JPEG залишилися більш круті, ніж для GaussianBlur, що підтверджує чутливість суб'єктивного сприйняття до високочастотних спотворень.

Зниження PSNR у середньому –0.35 дБ і SSIM –0.006 вказує на те, що адаптивний LSB у вибраній реалізації не вносить візуально помітних артефактів навіть на фоні наявних спотворень. Таким чином, вплив на якість не критичний. Семантика також зберігається – у зображеннях з високим MOS (більше 5.0) структура та ключові об'єкти залишаються розпізнаваними. Це означає, що приховані дані не вплинули на інтерпретацію сцени.

Щодо чутливості до типу спотворень. Для випадку зашумлення GaussianNoise зниження MOS після вбудовування було трохи більшим, ніж для розмиття GaussianBlur, що пояснюється взаємодією LSB-модифікації з шумовими пікселями, які більш відчутно спотворюють дрібні

деталі. Зв'язок MOS з об'єктивними метриками після вбудовування майже не змінився, що підтверджує стабільність адаптивного LSB відносно сприйняття. Таким чином, навіть на зображеннях із вже зниженим MOS, вбудовування великого тексту ("Заповіту") можливе без критичної втрати семантичної інформації, що важливо для систем прихованої передачі даних, орієнтованих на візуальне сприйняття людиною.

Висновки

У роботі проведено порівняльний аналіз методів приховування інформації в просторовій області з точки зору досягнення оптимального балансу між непомітністю приховування та стійкістю до можливих атак, а також визначення найефективніших підходів для практичного застосування в системах захисту інформації. Встановлено, що метод вбудовування у найменш значущий біт демонструє найвищі значення PSNR і SSIM. Це свідчить про майже непомітне візуально вбудовування, але потенційно менш стійке до атак (наприклад, JPEG-компресії). Методи псевдовипадкового інтервалу і псевдовипадкової перестановки дещо знижують візуальну якість, але підвищують стійкість за рахунок розподілу даних по зображенню. Значення параметрів ефективності, які обчислені для методів блокового приховування та заміни палітри – є компромісом між непомітністю та стійкістю. Метод квантування зображення та CJB мають нижчі значення PSNR і SSIM, оскільки змінюють більше пікселів, але забезпечують вищу стійкість до деяких методів опрацювання зображення. Внаслідок проведених досліджень встановлено, що врахування семантичного наповнення демонструє значно вищу якість прихованого передавання повідомлень, оскільки враховує не лише низькорівневі характеристики зображення, але й його змістовну структуру, що безпосередньо впливає на сприйняття людиною та складність виявлення. Семантичне наповнення є суттєвим фактором, що визначає ефективність стеганографічних методів.

Перелік посилань

1. Fridrich, J. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge: Cambridge University Press, 2009. 437 p. DOI: 10.1017/CBO9780511762800.
2. Zhang, Y., Luo, X., Guo, Y., Qin, C., Liu, F. Multiple robustness enhancements for image adaptive steganography in lossy channels // *IEEE Transactions on Circuits and Systems for Video Technology*. – 2020. – Vol. 30, No. 8. pp. 2750–2764. DOI: 10.1109/TCSVT.2019.2939315.
3. Журавель, Ю. І., Мичуда, Л. З. Методи підвищення непомітності та стійкості стеганоповідомлень із застосуванням фрактальних розмірностей // *Сучасний захист інформації*. 2025. № 1(61). С. 74–81. DOI: 10.31673/2409-7292.2025.011576.
4. Журавель, І. М., Мичуда, Л. З., Журавель, Ю. І. Підвищення ефективності стеганографічного методу приховування даних із застосуванням ітераційних функцій та додаванням шуму // *Український журнал інформаційних технологій*. 2021. Т. 3, № 2. С. 66–73. Режим доступу: <https://ujit.undip.org.ua/index.php/ujit/article/view/182>.
5. Hu, Y., Yang, Z., Cao, H., Huang, Y. Multi-modal steganography based on semantic relevancy // *International Workshop on Digital Watermarking*. Cham: Springer International Publishing, 2020. pp. 3-14. DOI: 10.1007/978-3-030-69325-6_1.
6. Zeng, L., Yang, N., Li, X., Chen, A., Jing, H., Zhang, J. Advanced image steganography using a U-Net-based architecture with multi-scale fusion and perceptual loss // *Electronics*. 2023. Vol. 12, No. 18. Article 3808. DOI: 10.3390/electronics12183808.
7. Liu, L., Meng, L., Wang, X., Peng, Y. An image steganography scheme based on ResNet // *Multimedia Tools and Applications*. 2022. Vol. 81, No. 27. pp. 39803-39820. DOI: 10.1007/s11042-022-13254-2.
8. Lu, H., Zhang, T. RobustStegFormer: A Cross-Attention Guided and Noise-Aware Transformer for Image Steganography // *6th International Conference on Computer Vision, Image and Deep Learning (CVIDL)*. IEEE, 2025. p. 617-621. DOI: (уточнюється після публікації).
9. Hu, D., Wang, L., Jiang, W., Zheng, S., Li, B. A novel image steganography method via deep convolutional generative adversarial networks // *IEEE Access*. 2018. Vol. 6. P. 38303–38314. DOI: 10.1109/ACCESS.2018.2852771.
10. Xie, G. Adaptive spatial image steganography and steganalysis using perceptual modelling and machine learning: Dissertation for the degree of Doctor of Philosophy. Guildford: University of Surrey, 2022. DOI: 10.15126/thesis.2022.001.
11. Ponomarenko, N., Lukin, V., Zelensky, A., Egiazarian, K., Carli, M., Battisti, F. TID2013 Image quality assessment database [Електронний ресурс]. 2013. Режим доступу: <https://www.ponomarenko.info/tid2013.htm>.

Надійшла 05.10.2025