https://doi.org/10.31649/1997-9266-2025-183-6-149-157

УДК 004.6.056(045)

Ю. Є. Яремчук[1]
О. В. Салієва[1]
В. С. Катаєв[1]
І. О. Бондаренко[1]
А. В. Галицький[1]

УДОСКОНАЛЕННЯ АЛГОРИТМУ ПРИХОВУВАННЯ ДАНИХ У ПРОСТОРОВУ ОБЛАСТЬ ІЗ ЗАСТОСУВАННЯМ ЗВАЖЕНОЇ ВЕКТОРНОЇ ФІЛЬТРАЦІЇ ТА СИНГУЛЯРНОГО СПЕКТРАЛЬНОГО АНАЛІЗУ

[1]Вінницький національний технічний університет

Сучасний стан розвитку інформаційних технологій вимагає впровадження високоефективних методів та засобів для забезпечення цілісності та конфіденційності цифрових даних. На сьогодні, разом з традиційними криптографічними методами захисту інформації особливого значення набувають стеганографічні підходи, основна перевага яких зумовлена здатністю приховувати не лише зміст даних, а й сам факт їхньої передачі. Серед стеганографічних методів найпоширенішими є методи вбудовування даних у просторову область растрових зображень, що пояснюється їхньою відносною простотою реалізації та низькою обчислювальною складністю. Разом з тим просторові стеганографічні методи є вразливими до різноманітних спотворень, таких як фільтрація, шумові атаки, ущільнення або інші операції обробки зображень, що призводить до зниження стійкості прихованої інформації та можливості її втрати. Це зумовлює необхідність удосконалення наявних методів з метою підвищення їхньої надійності та стійкості до зловмисних впливів. У зв'язку з цим, у роботі запропоновано модифікований стеганографічний алгоритм приховування інформації у просторову область із застосуванням зваженої фільтрації (Weighted Median Filter, WVF) та двовимірного сингулярного спектрального аналізу (2D-SSA), що дозволить ефективно виділити структурні компоненти зображення, підвищити стійкість вбудованих даних без суттєвого погіршення візуальної якості контейнерного зображення. До того ж запропонований метод розширено шляхом впровадження алгоритмів, спрямованих на зменшення впливу зашумлення (Gaussian, Salt & Pepper) та підвищення стійкості до ущільнення з використанням формату JPEG. Для оцінювання якості вбудованої інформації застосовано метрики PSNR і SSIM, які забезпечують можливість кількісного порівняння ефективності різних стеганографічних підходів, зокрема методів, що ґрунтуються на дискретному косинусному перетворенні (DCT) та заміні найменш значущих бітів (LSB). Додатково реалізовано механізм адаптивного вбудовування водяних знаків, що сприяє підвищенню надійності збереження прихованих даних в умовах реальних впливів.

Ключові слова: стеганографія, двовимірний сингулярний спектральний аналіз, зважений медіанний фільтр, зашумлення, ущільнення.

Вступ

В умовах інтенсивної цифровізації усіх сфер суспільного життя спостерігається зростання обсягів мультимедійного трафіку, що також висуває жорсткі вимоги до забезпечення конфіденційності та цілісності даних. Традиційні криптографічні засоби, спрямовані на шифрування змісту повідомлень, часто виявляються недостатніми, оскільки сам факт передачі зашифрованого трафіку може привернути увагу зловмисника. У цьому контексті вагомого значення набуває стеганографія, головною метою якої є маскування самої наявності секретної комунікації всередині візуально нейтральних цифрових об'єктів — контейнерів.

Найрозповсюдженішими у прикладній стеганографії є методи вбудовування даних у просторову область растрових зображень. Їхня популярність зумовлена високою пропускною здатністю та відносно низькою обчислювальною складністю реалізації. Проте головним недоліком таких підходів залишається низька стійкість до деструктивних впливів: адитивного шуму, операцій ущільнення, лінійної фільтрації та інших перетворень, що здатні спотворити або повністю знищити приховане повідомлення.

Одним з перспективних підходів до вирішення зазначеної проблеми є перехід від простого

вбудовування до адаптивних методів, що враховують структурні та текстурні особливості контейнера. У межах цього дослідження пропонується вдосконалити стеганографічний метод шляхом інтеграції апарату двовимірного сингулярного спектрального аналізу та зваженого медіанного фільтра. Адже використання 2D-SSA дозволяє здійснити декомпозицію зображення на структурні компоненти, що надає можливість ідентифікувати найстійкіші ділянки для вбудовування бітів інформації. У свою чергу, застосування WMF спрямоване на підвищення захищеності системи від зашумлення та фільтраційних атак. На відміну від стандартних фільтрів, WMF забезпечує кращу збереженість контурів та дрібних деталей зображення, що дозволяє мінімізувати візуальні артефакти після вбудовування та підвищити стійкість прихованих даних без суттєвої втрати якості стего-об’єкта.

Аналіз проблеми та постановка задачі

Дослідження питань щодо удосконалення стеганографічних методів описано у безлічі наукових праць. Так, у статті [1] запропоновано підхід для покращення стеганографічних методів, що базується на виявленні ділянок з високою фрактальною розмірністю для вбудування інформації з мінімальними візуальними спотвореннями та підвищеною стійкістю до зовнішніх впливів. Автори роботи [2] розробили новий стеганографічний метод вбудовування зображень у просторовій області, який базується на заміні найменш значущих бітів (LSB) і дозволяє вбудовувати секретні дані в RGB-зображення без помітних спотворень. На основі генеративно-змагальної мережі (GAN) в [3] побудовано нову просторову стеганографічну схему з механізмом перехресного зворотного зв’язку. У науковій праці [4] запропоновано новий підхід до локалізації корисного навантаження для класичних стеганографічних алгоритмів JSteg і F5, які реалізують вбудовування інформації у DCT-області. Цей метод ґрунтується на аналізі зображення-контейнера з подальшим зважуванням залишків DCT-коефіцієнтів відповідно до текстурних характеристик локальних областей, оцінених за допомогою локальної дисперсії, що забезпечує помітне підвищення точності локалізації. На основі рекомендацій PRISMA-ScR у роботі [5] проаналізовано стеганографічні методи приховування інформації у просторову область. Авторами праці [6] створено ключову стеганографічну систему, у якій досягнуто оптимізацію балансу між місткістю вбудованої інформації та показниками якості стего-об’єкта, а також зменшено ймовірність виявлення прихованих даних. У статті [7] детально проаналізовано відомі методи просторової стеганографії, такі як метод заміни бітів (LSB) та метод розширення різниці пікселів, а також зазначено їх переваги та недоліки.

Незважаючи на значну кількість наукових праць, щодо удосконалення стеганографічних підходів, залишається вагомим питання забезпечення стійкості до спотворень, що виникають унаслідок активних атак, за умови збереження прийнятної якості зображення. Одним із перспективних методів підвищення стійкості прихованої інформації є застосування двовимірного сингулярного спектрального аналізу, який надає змогу розділяти зображення на складові з різними частотними характеристиками. Такий підхід створює сприятливі умови для надійного вбудовування даних і забезпечує високий рівень їх збереження навіть за наявності значних зовнішніх впливів. До того ж додатковим механізмом для підвищення стійкості є застосування зваженого медіанного фільтра, який забезпечує зменшення рівня шуму та інших спотворень, спричинених активними атаками. Поєднання WMF з алгоритмом 2D-SSA сприяє надійному збереженню прихованої інформації, водночас обмежуючи негативний вплив атак на якість її відновлення. Тому актуальною задачею є розробка алгоритмічних засобів на основі методів двовимірного сингулярного спектрального аналізу та зваженого медіанного фільтра, що призначені для виокремлення структурних компонентів зображення, зниження рівня шумових спотворень і підвищення ефективності обробки та захисту прихованих даних. Вдосконалений алгоритм доцільно протестувати для визначення його стійкості до різних класів атак, а також оцінювання впливу на візуальні характеристики зображень.

Таким чином, *метою роботи* є розробка модифікованого стеганографічного алгоритму, який завдяки поєднанню можливостей 2D-SSA та фільтраційних властивостей WMF забезпечуватиме оптимальний баланс між місткістю, візуальною непомітністю та підвищеною стійкістю до зовнішніх впливів у просторовій області растрових зображень.

Удосконалення алгоритму 2D-SSA

Алгоритм 2D-SSA розширює сингулярний спектральний аналіз на двовимірні дані, наприклад, для аналізу зображень. Він забезпечує виділення основних компонентів зображення, зокрема, тренди та періодичні структури, а також ефективне зниження рівня шуму для покращення аналізу та якості обробки даних.

Основними етапами роботи досліджуваного алгоритму є: побудова матриці траєкторій, що містить інформацію про локальні структури зображення, представлені окремими рядками чи стовпцями, кожен з яких можна розглядати як незалежну частину; сингулярний розклад матриці у вигляді набору власних значень та векторів, які визначають вагу окремих компонент; групування отриманих компонентів та відновлення зображення на основі відфільтрованої матриці.

На рис. 1 показано удосконалений алгоритм 2D-SSA.

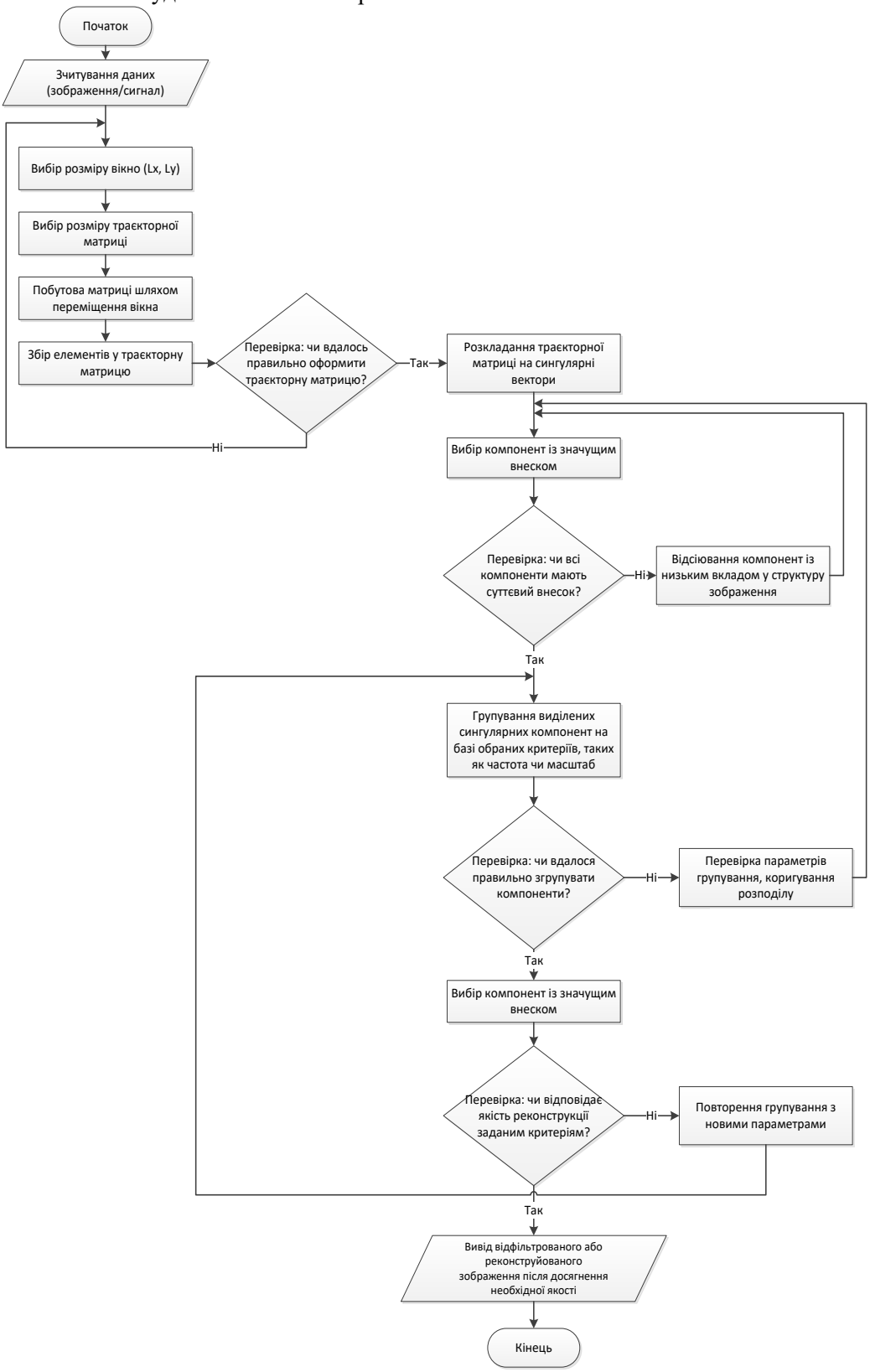

Рис. 1. Схема вдосконаленого алгоритму 2D-SSA

Опишемо роботу вдосконаленого алгоритму 2D-SSA.

Крок 1. Вибір параметрів.

Задається розмір вікна $\left(L_x, L_y\right)$, що визначає область аналізу зображення та рівень деталізації локальних структур. З урахуванням цих параметрів формується траєкторна матриця відповідної розмірності $\left(L_x \times L_y\right)$.

Крок 2. Формування матриці траєкторій.

Процедура формування матриці траєкторій полягає у послідовному накладанні вікна розміром $\left(L_x, L_y\right)$ на зображення зі зсувом на один піксель. Дані з кожного розташування вікна агрегуються у вектори, що утворюють стовпці матриці $\overline{X}$, яка відображає локальні фрагменти зображення розміром $\left(L_x \times L_y\right)$.

Крок 3. Сингулярний розклад матриці.

Здійснюється сингулярний розклад матриці $\overline{X}$, який дозволяє ідентифікувати ключові компоненти шляхом аналізу сингулярних значень та векторів.

Розклад траєкторної матриці за сингулярними значеннями задається формулою

$$\overline{X} = U\Sigma V^T,$$

де U та V — матриці, утворені лівими та правими сингулярними векторами; Σ — діагональна матриця, що містить сингулярні значення.

Крок 4. Вибір компонентів.

Компоненти з найбільшими сингулярними значеннями відповідають основному інформаційному вмісту зображення, зокрема, його структурні та періодичні характеристики. Компоненти з незначними значеннями, що зазвичай описують випадковий шум, вилучаються.

Крок 5. Формування груп.

Відібрані сингулярні компоненти об’єднуються у групи з метою відновлення зображення, що не містить шумових компонентів. Зазвичай, компоненти, що характеризуються подібними просторовими або періодичними властивостями, формують однин кластер.

Крок 6. Відновлення зображення.

На основі сформованих груп шляхом зворотного перетворення вибраних сингулярних векторів здійснюється відновлення зображення. Об’єднання реконструйованих компонентів дозволяє отримати зображення з мінімальним рівнем шуму або з акцентуванням періодичних структур.

Удосконалення алгоритму зваженого векторного медіанного фільтра (WVF)

WVF є нелінійним інструментом фільтрації, який застосовується для підвищення якості зображень і сигналів шляхом ефективного зменшення шуму зі збереженням ключових візуальних ознак, таких як межі зображення. WVF виявляє високу ефективність в умовах активних атак, що супроводжуються цілеспрямованими або агресивними шумовими спотвореннями.

Проаналізуємо ключові кроки функціонування модифікованого алгоритму зваженої векторно-медіанної фільтрації.

Крок 1. Формування вхідної вибірки.

На вхід алгоритму подається зображення у вигляді матриці пікселів або сигнал представлений у векторній формі $X = \{x_1, x_2, ...x_n\}$, де x_i відповідає окремому пікселю або елементу вибірки. Кожному елементу x_i призначається вага w_i, що може залежати від просторових характеристик або інтенсивності сигналу, забезпечуючи адаптацію фільтра до аномальних впливів чи атак.

Крок 2. Обчислення сумарних зважених відстаней.

Для кожного елемента x_i визначається сума зважених відстаней до інших елементів у межах фільтрувального вікна

$$D\left(x_i\right) = \sum_{(j=1)}^{n} w_j \cdot d\left(x_i, x_j\right),$$

де $d\left(x_i, x_j\right)$ — відстань між x_i та x_j.

Визначення вагових коефіцієнтів w_i здійснюється на основі показників, які мінімізують деструк-

тивний вплив активних атак на результати аналізу.

Крок 3. Визначення зваженої медіани.

Після сортування елементів за величинами $D(x_i)$ вибирається зважений медіанний елемент, що мінімізує суму зважених відстаней

$$WM = \arg min_{(x_i)} \sum_{(j=1)}^{n} w_j \cdot d(x_i, x_j).$$

Отримане значення використовується як заміна поточного елемента, зменшуючи вплив аномалій.

Крок 4. Заміна елементів.

Поточні елементи x_i замінюються обчисленим медіанним значенням, що забезпечує збереження контурів та видалення шуму чи атакованих пікселів.

Крок 5. Ітеративна обробка (за потреби).

Для підвищення стійкості до складних типів атак процедуру фільтрації можна повторити з оновленими ваговими коефіцієнтами. Результатом є очищене зображення або сигнал зі збереженням ключових елементів та країв.

Блок-схема роботи вдосконаленого алгоритму WVF показана на рис. 2.

Рис. 2. Блок-схема вдосконаленого алгоритму WVF

Оцінювання ефективності роботи вдосконаленого алгоритму

За результатами дослідження здійснено програмну реалізацію декількох стеганографічних алгоритмів, призначених для прихованого вбудовування водяних знаків у зображення. Зокрема, реалізовано такі алгоритми як: DCT — водяний знак інтегрується у низькочастотну складову зображення-носія; LSB — водяний знак вбудовується в найменш значущі біти зображення, забезпечуючи мінімальні візуальні спотворення; Adaptive DCT — реалізує вбудовування водяного знаку в контурні області зображення, що підвищує його стійкість до зашумлення та ущільнення.

Розроблена програмна моделює реальні умови обробки зображень шляхом додавання таких шумів як Gaussian Noise та Salt & Pepper. Окрім цього, виконується JPEG- ущільнення зображення з метою оцінювання стійкості вбудованого водяного знака після зазначених перетворень (рис. 3).

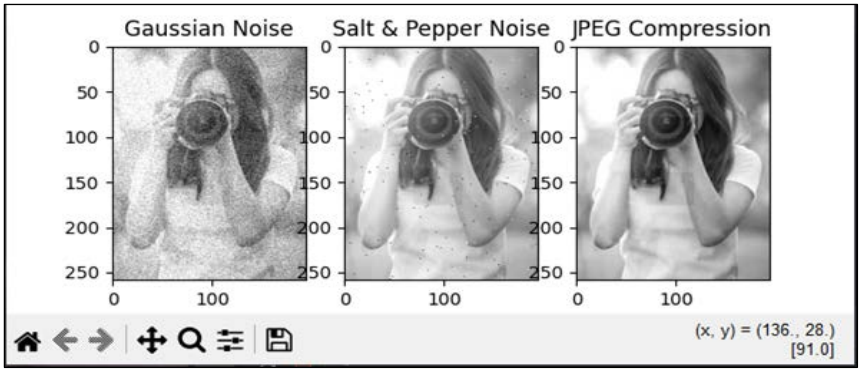

Рис. 3. Зашумлення методами Gaussian Noise та Salt & Pepper Noise

Для оцінювання якості зображень після вбудовування водяного знака та аналізу рівня внесених спотворень у програмі застосовуються метрики SSIM та PSNR (рис. 4).

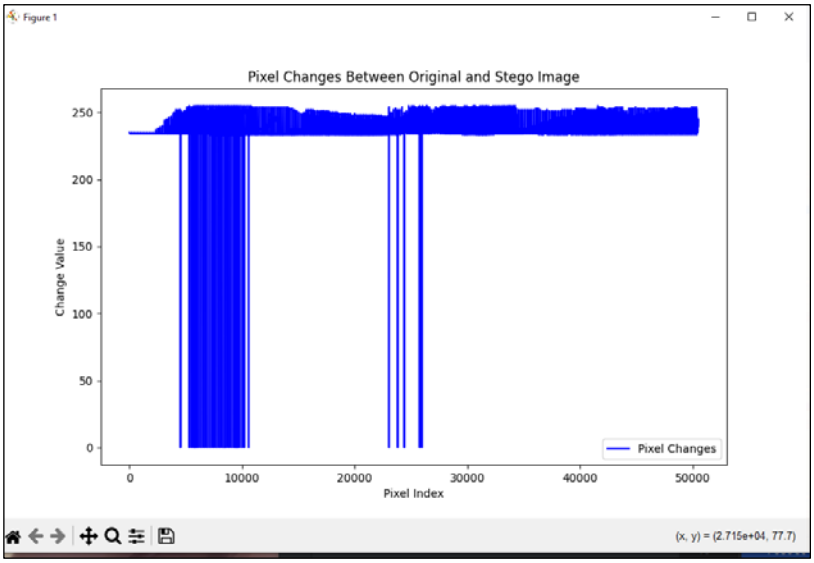

Рис. 4. Оцінювання значень пікселів оригінального та модифікованого зображення

На рис. 4 показано абсолютну зміну значень пікселів зображення після впливу шумів Gaussian Noise та Salt & Pepper, з нього ми чітко бачимо два різні патерни, що відповідають специфіці вказаних шумів, а саме: основний «масив» синього кольору, який ми бачимо у верхній частині (діапазон 230…250) — це вплив Gaussian Noise, що додає до кожного пікселя випадкове значення, яке розподілене за нормальним законом та вертикальні лінії, які різко падають до 0 (на відрізках 5000…10000 та 23000…26000) — це прояв Salt & Pepper Noise, що проявляється як різке встановлення значення пікселя в екстремальний мінімум (0 — чорна точка, «перець») або максимум (255 — біла точка, «сіль»).

По завершенні вбудовування водяного знаку здійснюється обчислення різниці між вихідним та стеганографічним зображеннями. Побудований графік ілюструє зміну значень пікселів у результаті застосування кожного з алгоритмів (рис. 5).

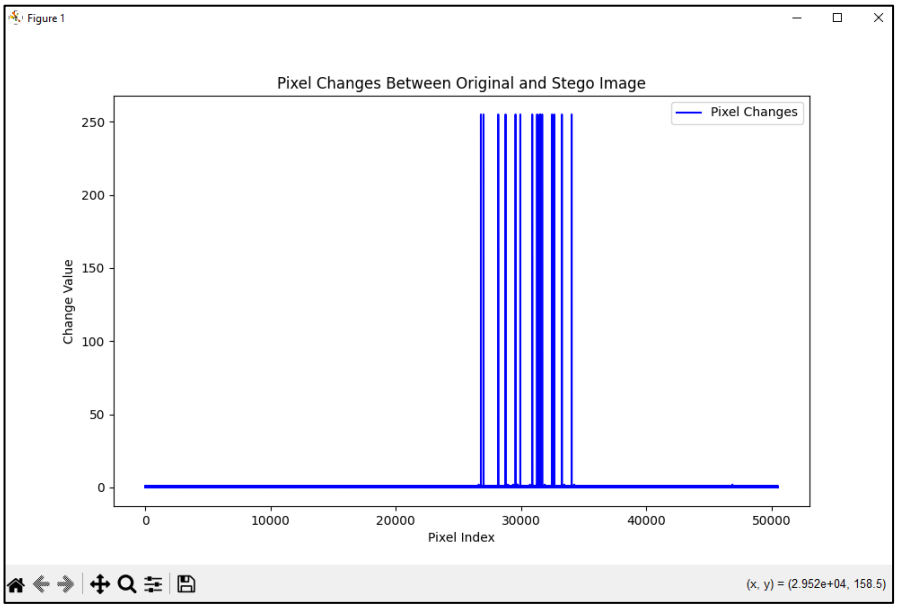

Рис. 5. Графік розподілу змін інтенсивності пікселів

LSB на графіку — це суцільна синя лінія у нижній частині графіка, зміни значень пікселів не перевищують 1—2 одиниці (зміна лише 1-го або 2-х найменш значущих бітів). Числові показники: PSNR найвищий серед усіх методів (>50 дБ), оскільки модифікації мінімальні, SSIM також має високе значення (~0,99), оскільки структура зображення майже не змінюється.

DCT на графіку помітний як невеликі «збурення», що можна побачити по всій довжині графіка (маленькі піки, що трохи вищі за 1). Числові показники: PSNR нижчий, ніж у LSB (>20 дБ), через масовість дрібних змін у багатьох пікселях, SSIM також нижчий (~0,96).

Adaptive DCT на графіку створює різкі вертикальні піки (до 255) у центральній частині (індекси пікселів 28,000…35,000), ці різкі сплески вказують на те, що алгоритм вибрав специфічні ділянки зображення для інтенсивного вбудовування даних. Числові показники: PSNR майже такий як у LSB (>50 дБ), а SSIM найкращий серед інших методів (>0,99).

Проаналізуємо результати експериментальних досліджень.

1. Оцінювання здатності алгоритмів коректно вбудовувати водяний знак за різних умов.

Програмний засіб апробовано на зображеннях з різними характеристиками, зокрема різної роздільної здатності та рівня деталізації. Результати експериментів показали, що всі розглянуті методи забезпечують вбудовування водяного знаку з незначними спотвореннями, що підтверджується високими значеннями метрик SSIM та PSNR.

2. Перевірка стійкості до шумових впливів і ущільнення.

Досліджувані алгоритми протестовано в умовах додавання шуму.

За наявності Gaussian Noise водяний знак краще зберігався за використання адаптивного DCT, що пояснюється його орієнтацією на крайові області зображення.

У разі впливу шуму типу Salt and Pepper спотворення спостерігались у всіх методах, проте DCT виявився найстійкішим.

Після застосування JPEG- ущільнення адаптивний DCT забезпечив кращу збереженість вбудованого водяного знаку.

3. Оцінювання ефективності за метриками PSNR та SSIM.

Метод DCT забезпечує високу якість зображення після вбудовування водяного знаку, що відображається у високих значеннях PSNR та SSIM.

Метод LSB демонструє нижчу ефективність у разі ущільнення, оскільки маніпуляції з найменш значущими бітами є вразливими до змін.

Адаптивний DCT характеризується найвищою стійкістю до шуму та ущільнення, хоча в окремих випадках може призводити до незначного зменшення PSNR через модифікації крайових елементів.

4. Аналіз отриманих результатів.

На рис. 6 подано результат проведеного аналізу досліджуваних методів.

```
Select carrier image:
Select watermark image:
DCT PSNR: 22.53161702881205, SSIM: 0.9631874169207203
LSB PSNR: 51.14824663905824, SSIM: 0.9979678176161669
Adaptive DCT PSNR: 51.12299738806085, SSIM: 0.9981219858601876
```

Рис. 6. Результат аналізу досліджуваних методів в консолі

Таким чином, адаптивний метод DCT виявився найстійкішим до шумів та спотворень, завдяки чому він є оптимальним вибором для приховування водяного знаку в реальних умовах.

Висновки

В результаті проведеного дослідження встановлено, що інтеграція зваженої векторної медіанної фільтрації (WVF) з двовимірним сингулярним спектральним аналізом (2D-SSA) підвищує стійкість прихованих даних у растрових зображеннях до активних атак. Адже, використання 2D-SSA дозволяє ефективно виділяти інформативні складові зображення, що створює умови для надійного та малопомітного вбудовування даних. Додаткове використання зваженого медіанного фільтра сприяє зменшенню викривлень, спричинених зовнішніми впливами, та збереженню структурних характеристик закодованої інформації.

Для оцінювання якості прихованої інформації у роботі використовувалися показники SSIM та PSNR, що дозволили порівняти ефективність різних стеганографічних методів, таких як DCT та LSB. У ході дослідження створювалися графіки змін пікселів, що демонструють точність та надійність алгоритму після обробки зображень. Проведено серію тестувань і оцінювання продуктивності методу на цифрових зображеннях різних форматів. Проведення тестування дало змогу встановити, що завдяки високій стійкості до спотворень та шумових впливів, адаптивний DCT є найефективні-

шим підходом для приховування водяного знаку у практичних умовах.

Отже, вдосконалений алгоритм може бути інтегрований в різні галузі суспільного життя, забезпечуючи ефективний захист даних та інтелектуальної власності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Ю. І. Журавель, і Л. З. Мичуда, «Методи підвищення непомітності та стійкості стеганоповідомлень із застосування фрактальних розмірностей,» *Сучасний захист інформації*, № 1, с. 74-81, 2025. https://doi.org/10.31673/2409-7292.2025.011576 .

[2] R. Shmueli, et al., "A novel technique for image steganography based on maximum energy seam," *Multimed Tools and Applications* 83, no. 28, pp. 70907-70920, 2024. https://doi.org/10.1007/s11042-024-18476-6 .

[3] F. Li, Z. Yu, and C. Qin, "GAN-based spatial image steganography with cross feedback mechanism," *Signal Processing*, no. 190, pp. 108341, 2022. https://doi.org/10.1016/j.sigpro.2021.108341 .

[4] B. Pan, et al., "Novel hidden bit location method towards JPEG steganography," *Security and Communication Networks*, vol. 2022, no. 1, pp. 8230263, 2022. https://doi.org/10.1155/2022/8230263 .

[5] D. Raghuvanshi, et al., "Advancing image steganography: PRISMA-ScR based analysis of spatial domain techniques," *Multimedia Tools and Applications*, pp. 1-35, 2025. https://doi.org/10.1007/s11042-025-21040-5 .

[6] P. Milosav, M. Milosavljevic, and Z. Banjac, "Steganographic method in selected areas of the stego-carrier in the spatial domain," *Symmetry*, vol. 15, no. 5, pp. 1015, 2023. https://doi.org/10.3390/sym15051015.

[7] A. M. Alhomoud, "Image steganography in spatial domain: Current status, techniques, and trends," *Intell. Autom. Soft. Comput.*, vol. 27, no. 1, pp. 2213-2224, 2021. https://doi.org/10.32604/iasc.2021.014773 .

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 17.12.2025

Яремчук Юрій Євгенович — д-р техн. наук, професор, професор кафедри менеджменту та безпеки інформаційних систем, e-mail: yurevyar@vntu.edu.ua ;

Салієва Ольга Володимирівна — д-р філософії, доцент кафедри менеджменту та безпеки інформаційних систем, e-mail: salieva8257@ vntu.edu.ua ;

Катаєв Віталій Сергійович — асистент кафедри менеджменту та безпеки інформаційних систем, e-mail: kataev@vntu.net ;

Бондаренко Ірина Олексіївна — асистент кафедри менеджменту та безпеки інформаційних систем, e-mail: fm.ub15b.bondarenko@gmail.com ;

Галицький Артур Валентинович — студент магістратури кафедри менеджменту та безпеки інформаційних систем, e-mail: artur.galitskiy.2019@gmail.com .

Вінницький національний технічний університет, Вінниця

Yu. Ye. Yaremchuk[1]
O. V. Saliieva[1]
V. S. Kataiev[1]
I. O. Bondarenko[1]
A. V. Halytskyi[1]

Enhancement of a Spatial Domain Data Hiding Algorithm Using Weighted Vector Filtering and Singular Spectrum Analysis

[1]Vinnitsa National Technical University

The current state of information technology development necessitates the implementation of highly effective methods and tools to ensure the integrity and confidentiality of digital data. Today, alongside with the traditional cryptographic methods of information protection, steganographic approaches are gaining particular importance, as their main advantage lies in the ability to conceal not only the content of the data but also the very fact of its transmission. Among steganographic methods, the most widely used are techniques for embedding data in the

spatial domain of raster images, which is explained by their relative ease of implementation and low computational complexity. At the same time, spatial steganographic methods are vulnerable to various distortions such as filtering, noise attacks, compression, or other image processing operations, which can reduce the robustness of hidden information and increase the risk of data loss. This highlights the need to improve existing methods to enhance their reliability and resilience against malicious impacts.

In this regard, the present work proposes a modified steganographic algorithm for information hiding in the spatial domain using Weighted Median Filtering (WMF) and Two-Dimensional Singular Spectrum Analysis (2D-SSA). This approach allows effective extraction of structural components of the image and improves the robustness of embedded data without significantly degrading the visual quality of the cover image. Furthermore, the proposed method has been extended by incorporating algorithms aimed at reducing the effects of noise (Gaussian, Salt & Pepper) and enhancing robustness against JPEG compression. To assess the quality of the embedded information, PSNR and SSIM metrics were applied, enabling quantitative comparison of the efficiency of different steganographic approaches, including methods based on Discrete Cosine Transform (DCT) and Least Significant Bit (LSB) substitution. Additionally, an adaptive watermark embedding mechanism has been implemented, which further enhances the reliability of hidden data preservation under real-world conditions.

Keywords: steganography, two-dimensional singular spectrum analysis, weighted median filter, noise, compression.

Yaremchuk Yurii Ye. — Dr Sc. (Eng.), Professor, Professor of the Chair of Management and Information Systems Security, e-mail: yurevyar@vntu.edu.ua ;

***Saliieva Olha V.* —** PhD, Associate Professor of the Chair of Management and Information Systems Security, e-mail: salieva8257@vntu.edu.ua ;

***Kataiev Vitalii S.* —** Assistant of the Chair of Management and Information Systems Security, e-mail: kataev@vntu.net ;

***Bondarenko Iryna O.* —** Assistant of the Chair of Management and Information Systems Security, e-mail: fm.ub15b.bondarenko@gmail.com ;

***Halytskyi Artur V.* —** Master's Student of the Chair of Management and Information Systems Security, e-mail: artur.galitskiy.2019@gmail.com