УДК 004.056.1:004.8

В. В. Карпінець, канд. техн. наук, доц.; Д. П. Присяжний; К. В. Безпалий; В. М. Білоус; Д. В. Тельнік

УДОСКОНАЛЕНИЙ ПІДХІД ДО ФОРМУВАННЯ СТЕГАНОКОНТЕЙНЕРІВ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Роботу присвячено підвищенню стійкості стеганографічних систем до пасивних атак шляхом удосконалення підходу до формування стеганоконтейнерів. Актуальність дослідження зумовлена тим, що більшість наявних методів приховування даних використовують готові цифрові зображення, статистичні характеристики яких не враховують подальше вбудовування інформації. У результаті модифікація частотних коефіцієнтів може призводити до появи аномалій, що виявляються сучасними засобами стеганоаналізу. Особливо це стосується випадків, коли структура текстурних зон зображення є нерівномірною або має недостатній рівень інформаційної надлишковості.

У роботі запропоновано підхід, що передбачає попередній синтез зображення-контейнера із заданими властивостями з подальшим вбудовуванням у нього секретних даних. Для генерації адаптивних носіїв використано можливості системи штучного інтелекту Midjourney. Формування контейнера здійснюється на основі підготовлених запитів, які дозволяють керувати складністю текстури, рівнем деталізації, контрастністю та загальним характером частотного розподілу.

Такий підхід дає змогу отримувати зображення, структура яких є більш придатною для приховування інформації без суттєвого порушення природних статистичних закономірностей. Вбудовування даних реалізовано за методом Коха-Жао з використанням дискретного косинусного перетворення. Процес передбачає поділ зображення на блоки, перехід до частотної області та модифікацію відносної різниці середньочастотних коефіцієнтів. Вибір саме цієї області обумовлений компромісом між непомітністю змін і стійкістю до JPEG-компресії. При цьому враховуються особливості зорової системи людини, зокрема знижена чутливість до спотворень у текстурованих ділянках та ефекти просторового маскування.

Експериментальні дослідження включали порівняння запропонованого підходу з традиційним вбудовуванням у випадково обрані зображення. Оцінювання проводилося за показниками візуальної якості, аналізом піксельної структури та дослідженням частотних характеристик.

Отримані результати свідчать про зменшення статистичних відхилень і підвищення стійкості до пасивного виявлення за збереження прийнятного рівня візуальної якості.

Ключові слова: *стеганоконтейнер, пасивні атаки, штучний інтелект (ШІ), Midjourney, дискретне косинусне перетворення, зорова система людини.*

Вступ

У задачах захисту інформації дедалі більшого значення набувають методи, що дозволяють приховати не лише зміст повідомлення, а й сам факт його передавання. До таких методів належить стеганографія, яка передбачає вбудовування даних у цифрові об'єкти таким чином, щоб модифікації залишалися непомітними для людини та складними для виявлення засобами аналізу. Найпоширенішим типом носіїв є цифрові зображення. Це зумовлено їх значним обсягом даних, наявністю текстурованих областей та особливостями зорової системи людини, яка менш чутлива до незначних локальних спотворень. Проблема полягає в тому, що ефективність стеганосистеми визначається не лише стійкістю до активних атак, але й здатністю протидіяти пасивному стеганоаналізу. У випадку, коли сам факт наявності прихованої інформації виявлено, систему вважають скомпрометованою. Сучасні методи стеганоаналізу базуються на статистичному аналізі структурних характеристик зображення та виявленні відхилень від природних закономірностей. Використання стандартних, попередньо сформованих зображень як контейнерів не завжди забезпечує оптимальні умови для вбудовування, що підвищує ризик виявлення. Практичний інтерес становить підхід, за якого контейнер формується з урахуванням обсягу та параметрів секретних даних.

Застосування генеративних моделей штучного інтелекту дає змогу синтезувати зображення із заданими статистичними властивостями, після чого вбудовування інформації здійснюється у частотній області, зокрема за допомогою дискретного косинусного перетворення. Така комбінація дозволяє зменшити статистичні аномалії та підвищити стійкість до пасивного аналізу, забезпечуючи формування унікальних стеганоконтейнерів для кожного сеансу передавання.

Захист інформації від несанкціонованого доступу залишається актуальною задачею, у межах якої активно розвивається стеганографія – напрям, спрямований на приховування факту передавання повідомлення [1]. Стеганографічна система являє собою сукупність методів формування прихованого каналу шляхом вбудовування даних у цифровий носій.

Будь-яке стеганографічне перетворення ґрунтується на двох принципах: контейнер має допускати незначні зміни без втрати функціональності, а рівень внесених спотворень повинен залишатися нижчим за поріг їх виявлення. Як контейнери використовуються різні типи цифрових даних, зокрема зображення, у яких модифікації можуть здійснюватися в просторовій або частотній області [1].

Разом із тим ефективність приховування суттєво залежить від властивостей конкретного носія. Не всі зображення мають достатню інформаційну надлишковість для безпечного вбудовування даних, що підвищує ризик їх виявлення під час візуального або статистичного аналізу.

Методи вбудовування інформації в медіаносії (зображення, аудіо, відео) є основою стеганографії, оскільки дозволяють приховувати дані таким чином, щоб вони залишалися непомітними для стороннього спостерігача. У випадку цифрових зображень такі методи застосовуються для забезпечення конфіденційності, створення водяних знаків, підтвердження авторства тощо. Серед основних підходів [2] виділяють: методи заміни в просторовій області; методи приховування в частотній області; широкосмугові; статистичні; методи перекручування та структурні методи. Більш стійкими до спотворень, зокрема компресії, вважаються методи, що реалізуються у частотній області. Перехід до частотної області здійснюється за допомогою різних перетворень зображення-контейнера. Найпоширенішими є методи на основі дискретного косинусного перетворення, перетворення Фур'є, вейвлет-перетворення, перетворення Карунена-Лоева та інші [3]. Такі перетворення можуть застосовуватися як до всього зображення, так і до його окремих блоків, що дозволяє гнучко обирати область вбудовування та контролювати рівень внесених змін.

Разом із вибором способу вбудовування важливим є і підхід до формування самого контейнера. Методи створення стеганоконтейнерів мають враховувати мінімізацію статистичних ознак, які можуть бути використані для виявлення прихованих даних [4]. Конструюючі підходи, що передбачають генерацію контейнера під конкретний обсяг і тип повідомлення, зменшують можливість ідентифікації за типовими ознаками подібності [5]. Використання технологій штучного інтелекту для генерації таких контейнерів дозволяє формувати унікальні зображення зі заданими характеристиками. При цьому для протидії пасивним атакам доцільним є вбудовування інформації саме у частотній області, що забезпечує вищу стійкість до статистичного аналізу, хоча може дещо знижувати стійкість до активних впливів.

Динамічний розвиток методів цифрового аналізу даних зумовлює необхідність пошуку нових підходів до створення стеганоносіїв, здатних протидіяти сучасним пасивним атакам. Актуальність дослідження полягає у розробці методів генерації адаптивних контейнерів, структура яких мінімізує статистичні та візуальні відхилення при вбудовуванні конфіденційної інформації.

Метою роботи є вдосконалення методу генерування стеганографічних контейнерів на основі системи штучного інтелекту Midjourney для підвищення рівня захищеності даних від пасивних атак.

Для реалізації поставленої мети розроблено алгоритм інтелектуального синтезу зображень, що базується на врахуванні характеристик зорової системи людини та специфіки

частотної області носія. Новизна підходу полягає в автоматизації створення унікальних стеганоконтейнерів із заздалегідь визначеними властивостями, що забезпечує високу стійкість до виявлення порівняно з традиційними методами використання готових статичних зображень.

Практичне значення методу, що пропонується в роботі, полягає в автоматичному створенні безпечних зображень для прихованої передачі даних. Використання системи Midjourney дозволяє відійти від звичайних зображень, які не стійкі до пасивних атак. Кожен стеганоконтейнер створений з використанням ШІ та патернів користувача є унікальним за структурою, що ускладнює виявлення сторонніми особами передачу секретної інформації у загальному потоці даних.

Запропонований підхід може бути впроваджений у програми для захищеного листування або сервіси передачі медіафайлів. Застосування запропонованого методу також можливе при стисненні зображень і враховує особливості людського зору, тому зміни залишаються непомітними. Це перетворює захист даних на сучасну технологію, яка сама підбирає найбільш відповідні параметри зображення під конкретне повідомлення.

Виклад основного матеріалу

Результати проведених досліджень свідчать, що найстійкішими до пасивних атак є методи, що ґрунтуються на вбудовуванні даних у частотну область зображення.

У цій роботі авторами розглядається вдосконалення методу приховування даних шляхом оптимального вибору стеганоконтейнера. Для визначення найефективніших варіантів контейнерів доцільно проаналізувати особливості зорової системи людини (ЗСЛ).

Характеристики ЗСЛ традиційно поділяють на дві категорії:

– низькорівневі («фізіологічні»);

– високорівневі («психофізіологічні»).

Дослідження, опубліковані наприкінці минулого століття, зосереджені переважно на аналізі низькорівневих характеристик зору. Проте на сьогодні дедалі поширенішою є тенденція до розробки стеганоалгоритмів, які враховують саме високорівневі особливості сприйняття інформації людиною.

Розглянемо характеристики обох категорій детальніше:

У межах низькорівневої категорії виокремлюють три ключові властивості, що визначають помітність стороннього шуму (артефактів вбудовування) на зображенні: контрастну чутливість, частотну чутливість та ефект маскування:

– контрастна чутливість: згідно з законом Вебера, для середнього діапазону яскравості поріг нерозрізненості змін (ΔI) є приблизно постійним і становить:

$$\Delta I \approx (0{,}01 \,/\, 0{,}03) \cdot I.$$

Водночас у зонах дуже низької або дуже високої яскравості цей поріг зростає, що дозволяє вбудовувати більший обсяг даних у найтемніші та найсвітліші ділянки без візуальних спотворень.

– частотна чутливість: зорова система людини має нерівномірну амплітудно-частотну характеристику. Встановлено, що людина значно чутливіша до низькочастотних (НЧ) спотворень, ніж до високочастотного (ВЧ) шуму. Це обґрунтовує доцільність розміщення стеганоносія саме у високочастотних складових зображення.

– ефект маскування: дане явище полягає у підвищенні порогу виявлення цільового сигналу за наявності іншого (маскувального) сигналу зі схожими характеристиками. Це зумовлено тим, що компоненти зображення з близькими параметрами активують одні й ті самі нейронні підканали ЗСЛ.

Ефект маскування є найбільш вираженим на текстурованих (високочастотних) ділянках із хаотичною структурою. На противагу цьому, на однотонних (низькочастотних) фрагментах адитивний шум стає критично помітним через відсутність маскувальних перешкод.

На відміну від низькорівневих ознак, високорівневі властивості ЗСЛ на сьогодні рідко

інтегруються в стеганографічні алгоритми, хоча вони відіграють вирішальну роль у процесі візуального сприйняття. Їхня специфіка полягає в когнітивній обробці первинної зорової інформації, на основі якої мозок здійснює адаптивне фокусування уваги на окремих фрагментах зображення.

Основними показниками, що визначають візуальну пріоритетність об'єктів, є:

– контрастна чутливість: ділянки з високим локальним контрастом та різкими перепадами яскравості першочергово привертають увагу спостерігача, що робить їх критично чутливими до внесення стеганошуму:

– масштабна залежність: об'єкти більшого розміру є візуально значущішими порівняно з дрібними деталями; проте існує певний поріг насичення, після досягнення якого подальше збільшення площі об'єкта не призводить до лінійного зростання його помітності;

– чутливість до розміру: видовжені та тонкі структури викликають вищий рівень зорової фіксації порівняно з об'єктами округлої або однорідної форми;

– колірна чутливість: кремі спектральні діапазони (зокрема червоний колір) мають вищий пріоритет сприйняття, цей ефект посилюється за умови високого хроматичного контрасту між об'єктом та фоном;

– просторова локалізація: процес розглядання зображення характеризується вираженою орієнтацією на центр експозиції та об'єкти переднього плану, що робить периферійні ділянки та задній план менш вразливими до виявлення вбудованих даних;

– чутливість до зовнішніх подразників: стратегія руху очей спостерігача суттєво залежить від зовнішнього контексту, попередніх інструкцій та цільової установки під час перегляду контенту.

Аналіз властивостей зорової системи людини дозволяє визначити ключові чинники, що впливають на помітність сторонніх втручань у структуру зображення. На основі цих даних стає можливим синтез стеганоконтейнерів із оптимальними характеристиками. Основна ідея вдосконалення полягає в активному врахуванні високорівневих категорій зору, які зазвичай залишаються поза увагою під час побудови стеганографічних систем.

Для реалізації цього підходу запропоновано використовувати можливості штучного інтелекту, зокрема системи Midjourney. Процес побудований на перетворенні вимог до безпеки та особливостей сприйняття у набір правил, за якими генерується зображення-контейнер.

Використання генеративного ШІ забезпечує гнучке керування параметрами зображення через систему текстових запитів. Чим детальніше описано зміст та структуру зображення, тим ефективнішим є результат генерації. Такий підхід дозволяє цілеспрямовано коригувати:

– параметри об'єктів: вибір кольорів, розмірів та форм, що мінімізують візуальну помітність вбудованих даних;

– композицію: розміщення елементів таким чином, щоб відволікати увагу від зон вбудовування інформації.

Саме можливість впливу на високорівневе сприйняття людини є ключовим аспектом удосконалення наявних методів. Генерація зображень із заздалегідь визначеними властивостями дозволяє створювати контейнери, які є стійкими до виявлення та забезпечують надійний захист інформації від пасивних атак.

Далі детальніше опишемо процес генерації зображення та вбудовування даних у стеганоконтейнер на основі запропонованого вдосконалення.

Процес створення стеганоконтейнера за запропонованим підходом базується на взаємодії з системою Midjourney [9] за допомогою текстових запитів – промптів (prompts). Система інтерпретує слова та фрази, розбиваючи їх на окремі маркери (tokens), які слугують основою для синтезу зображення.

Ефективність генерації безпосередньо залежить від точності складеного запиту. Промпт може мати як просту структуру (окремі слова чи фрази), так і розширену, що включає:

– image prompts: посилання на URL-адреси зображень для задання стилістики;

– text prompts: безпосередній текстовий опис об'єктів та сцени;

– parameters: технічні команди в кінці запиту, що визначають пропорції, версію моделі та алгоритми масштабування.

Під час формування текстового опису слід дотримуватися принципу лаконічності: система краще сприймає конкретні іменники та прикметники, ніж складні граматичні конструкції. Наприклад, замість складного речення «покажи зображення квітів маку, що намальовані олівцями у яскраво-помаранчевому кольорі» доцільно вказати: «яскраво-помаранчеві маки, намальовані кольоровими олівцями».

Основними технічними критеріями, що враховуються під час генерації, є розмір, роздільна здатність, природність текстур та наявність достатньої кількості областей для вбудовування даних. Окрім технічних параметрів, запит формується з урахуванням особливостей сприйняття людини.

Для мінімізації уваги до контейнера під час формування промпту висуваються такі вимоги до зображення:

– контраст: обмеження різких перепадів яскравості;

– масштаб: уникнення масивних елементів на користь дрібних деталей;

– геометрія: пріоритет закруглених та однорідних форм над довгими й тонкими об'єктами;

– колористика: використання спокійної гами та обмеження агресивних кольорів (зокрема червоного);

– композиція: рівномірний розподіл об'єктів по площині для уникнення надмірної концентрації уваги в центрі або на передньому плані.

Синтез зображення з дотриманням цих критеріїв дозволяє отримати стеганоконтейнер, який заздалегідь підготовлений до приховування інформації та стійкий до візуального та статистичного аналізу.

Послідовність формування набору prompt-команд для генерації стеганографічних контейнерів наведена у вигляді схеми (рис. 1).

Рис. 1. Вимоги до формування інтелектуальних запитів для створення контейнерів

Для точнішого керування процесом генерування до текстового запиту додаються специфічні параметри, що визначають технічні та візуальні характеристики контейнера. Зокрема, варто відзначити такі ключові параметри:,

– параметр для визначення якості обробки (--quality або --q); встановлене значення --q 1 забезпечує максимальну деталізацію зображення, що необхідно для створення складної текстури, придатної для приховування даних.

– параметр для виключення небажаних об'єктів (--no), який дозволяє автоматично усувати елементи, що підвищують візуальну помітність вбудовування; для протидії пасивним атакам до параметра додаються інструкції щодо уникнення високого контрасту, великих акцентних елементів, складних форм та перенасиченого переднього плану: --no contrasts, big elements, complex forms, foreground.

До основної частини запиту також включаються описові слова для забезпечення високої

роздільної здатності (high resolution), великих розмірів (large sizes) та нейтральної колірної гами (pastel dull tones).

Структура підсумкового запиту має такий вигляд:

Prompt = <об'єкт зображення>, high resolution, large sizes, pastel dull tones, --q 1, --no contrasts, big elements, complex forms, foreground.

Приклад структури промпту наведено на рис. 2.

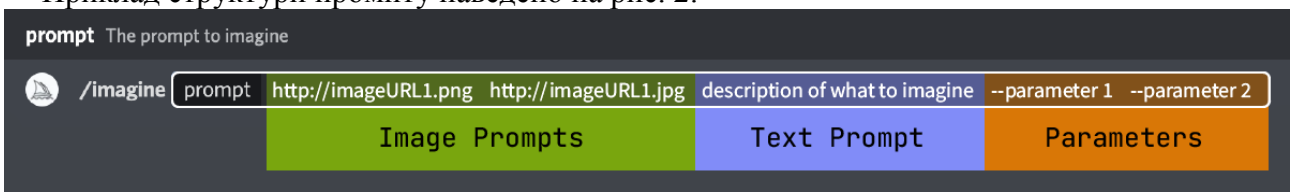
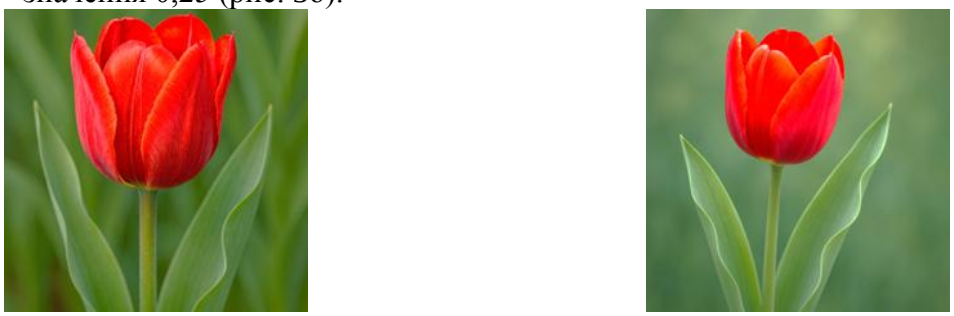


Рис. 2. Розширений формат формування prompts до нейромережі для вдосконалення генерації стеганоконтейнерів

Запропонована структура запиту є універсальною: користувач може обирати будь-яку предметну область (природа, архітектура, абстракція), проте незмінний набір параметрів та обмежень забезпечує стабільну стійкість згенерованого контейнера до методів пасивного стеганоаналізу. Це дозволяє суттєво мінімізувати візуальні спотворення та підвищити рівень захисту інформації порівняно з наявними методами.

Для демонстрації впливу параметрів генерації на очікуваний контейнер порівняємо результати декількох експериментів. У першому випадку проаналізуємо параметр --quality – створимо зображення об'єкту, щоб продемонструвати саме цей показник, а не генерацію контейнера в цілому. Для першої генерації встановимо цей параметр на рівні 1 (рис. 3а), а для другої – значення 0,25 (рис. 3б).



а) б)

Рис. 3. Експериментальне дослідження значення параметру--quality

Як можна побачити з отриманих результатів, зображення на рис. За демонструє вищу відповідність поставленій задачі – генерації максимально деталізованого об'єкта. Оскільки для формування стеганографічного контейнера критично важливо забезпечити високу якість носія, у подальшій роботі цей параметр встановлюється на рівні 1. Це дозволяє досягти високої роздільної здатності та збільшити корисну ємність контейнера для вбудовування секретних даних.

Наступний параметр, який було перевірено експериментальним шляхом – параметр --no. Його використання дозволяє вказати системі об'єкти або візуальні характеристики, яких слід уникати під час генерації. Параметр --no приймає кілька значень, розділених комами.

Для проведення експерименту було визначено наступний перелік обмежень:contrasts – виключення контрастних елементів із різкими переходами; bigelements – уникнення великих акцентних елементів; complexforms – відмова від складних геометричних форм; foreground – мінімізація акцентних деталей на передньому плані.

У результаті запит до системи містив наступну комбінацію: --nocontrasts, bigelements, complexforms, foreground. Додатково до текстової частини промпту було внесено уточнення щодо технічних характеристик:

– highresolution (висока роздільна здатність);

– largesizes (великий розмір);

– dulltones (приглушені кольори).

Результати експерименту наведено на рис. 4а (генерація без обмежень) та на рис. 4б (із застосуванням параметру --no).

Порівняльний аналіз отриманих зображень дозволяє візуально оцінити суттєву різницю. Оптимальним варіантом для приховування інформації та забезпечення стійкості до пасивних атак є саме друге зображення (рис. 4б). У ньому враховано ключові вимоги стеганографії: відсутність різких контрастів, складних форм та виражених акцентів.

Це дозволяє сформувати однорідну структуру носія, яка не привертає увагу потенційного зловмисника під час аналізу даних на наявність прихованих повідомлень.

а) б)

Рис. 4. Експериментальне дослідження значення параметру--no

Запропонований метод базується на інтелектуальному синтезі контейнерів та використанні дискретного косинусного перетворення (ДКП) для вбудовування даних у частотну область. Процес реалізації алгоритму складається з таких етапів:

Крок 1. Аналіз вхідних даних та визначення параметрів.

Визначення обсягу інформації, що потребує приховування та на основі цього розрахунок необхідної ємності, кількості та роздільної здатності стеганоконтейнерів. Вибір предметної області для генерації з метою забезпечення варіативності носіїв.

Крок 2. Формування та виконання запиту до нейромережі.

Створення формалізованого prompt-запиту з урахуванням технічних параметрів та характеристик ЗСЛ. Передача сформованого запиту до системи Midjourney для синтезу зображення.

Крок 3. Аналіз отриманого зображення на відповідність критеріям: достатність візуальної ємності для вбудовування, відсутність помітних артефактів та відповідність заданій тематиці. У разі невідповідності здійснюється повторна генерація (ітераційне повернення до Кроку 2).

Крок 4. Конвертація згенерованого зображення з формату PNG у JPEG, що є оптимальним для роботи з частотними коефіцієнтами. Дослідження частотної області контейнера для визначення зон, найбільш стійких до вбудовування.

Крок 5. Вбудовування даних у частотну область.

Застосування дискретного косинусного перетворення для переходу у частотну область зображення. Модифікація відповідних коефіцієнтів для приховування інформації та виконання зворотного перетворення для отримання фінального стегооб'єкта.

Структурну схему вдосконаленого алгоритму генерації та вбудовування даних представлено на рис. 5.

Ефективність запропонованого підходу оцінюється шляхом порівняльного аналізу показників спотворення оригінального зображення при використанні класичного методу Коха-Жао [10] та вдосконаленого методу на основі ШІ-генерації контейнерів.

В обох випадках секретні дані вбудовуються у частотну область зображення шляхом відносної зміни двох середньочастотних коефіцієнтів дискретного косинусного перетворення (ДКП). Вибір саме цих коефіцієнтів забезпечує стійкість інформації до JPEG-компресії та мінімізує видимі спотворення для зорової системи людини.

Основним критерієм порівняння є рівень візуальних спотворень при забезпеченні заданої стійкості стеганосистеми. Такий аналіз дозволяє підтвердити, що синтез адаптивного контейнера за допомогою штучного інтелекту забезпечує вищі показники прихованості порівняно з використанням випадкових зображень. Результати тестування наведено в табл. 1.

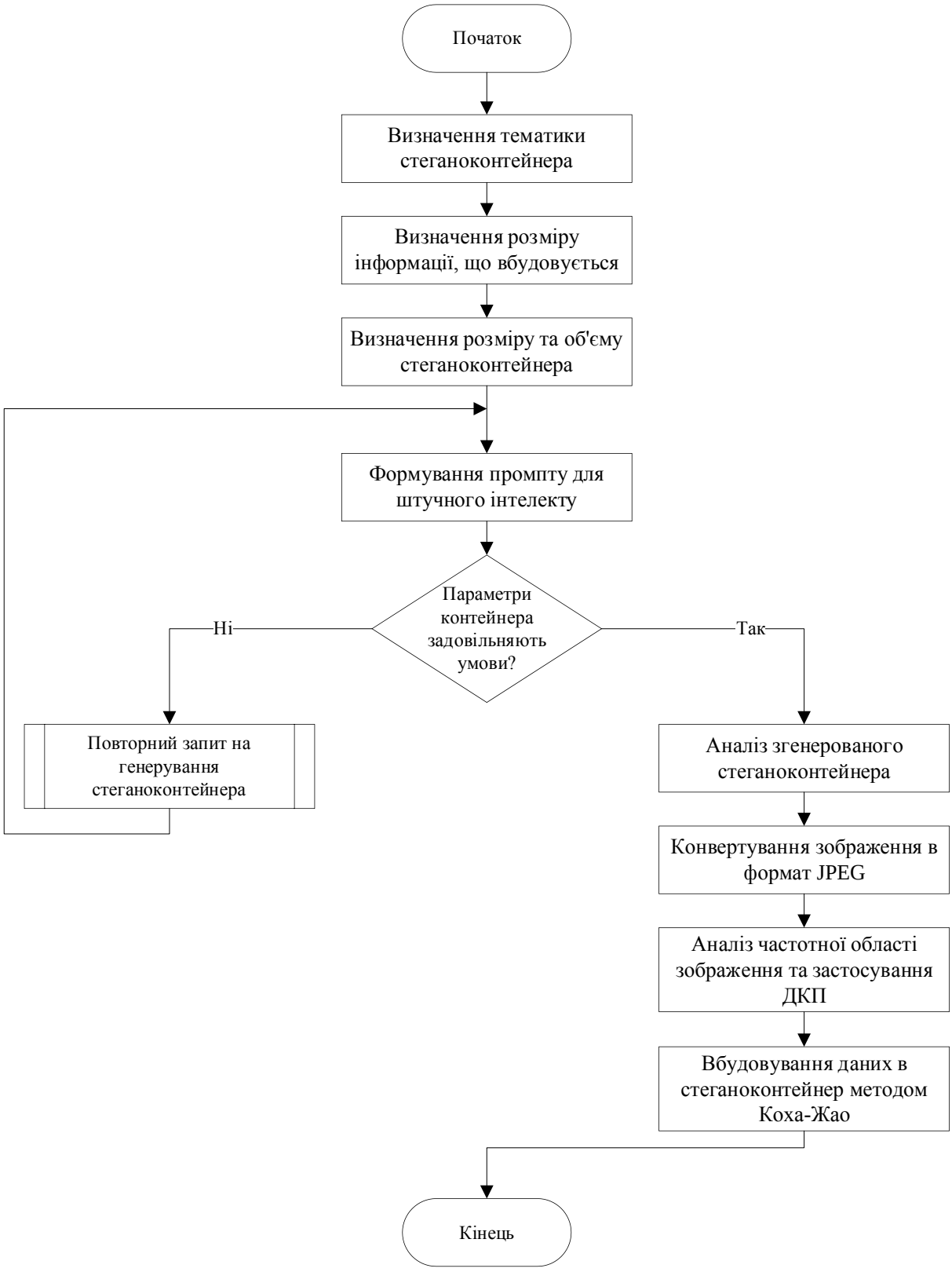


Рис. 5. Алгоритм генерації стеганоконтейнера та вбудовування даних

Для оцінки якості стеганоконтейнерів було використано показники, що базуються на аналізі піксельної структури зображення. Попри поширеність таких метрик, вони часто не повною мірою корелюють із особливостями людського зору. Саме тому в цій роботі акцент

зроблено на врахуванні чутливості до контрасту та ефекту маскування, що відповідає багатоканальній моделі зорового сприйняття.

Таблиця 1

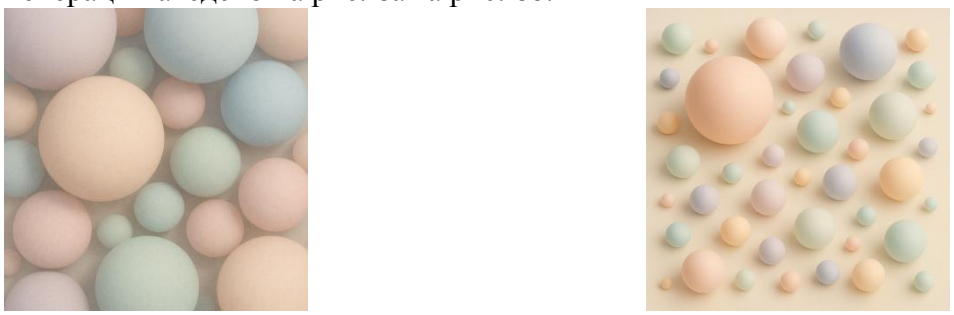
Порівняльна оцінка рівня візуальних спотворень у базовому та вдосконаленому методах

Назва показника спотворення	Оригінал	Коха-Жао (P = 0.5)	Коха-Жао з ШІ
Макс. абсолютна різниця, MD	0	39	33
Середня абсолютна різниця, AD	0	9,504	7,985
Норм. середня абс. різниця, NAD	0	0,074	0,061
Середньоквадр. помилка, MSE	0	124,383	123,1445
Нормована середньоквадр. помилка,NMSE	0	$5{,}065 \cdot 10^{-3}$	$4{,}895 \cdot 10^{-3}$
L^p-норма, p = 2	0	11,153	10,456
Лапласовасередньоквадр. помилка,LMSE	0	0,020	0,005
Відношення с/ш, SNR	∞	197,423	184,569
Макс. відношення с/ш,PSNR	∞	522,782	485,236
Якість зображення, IF	1	0,994935	0,99985
Норм. взаємна кореляція, NC	1	0,993261	0,99651
Якість кореляції, CQ	190,182	188,901	189,025
Структурний зміст, SC	1	1,0084484	1,00452
Загальне сигма-відношення с/ш,GSSNR	∞	87,792	92,163
Сигма відношення с/ш,SSNR	∞	72,9	76,5
Нормоване відношення с/ш помилка,NSER	256	100	114
Подібність гістограм, NS	0	11096	10452

Порівняльний аналіз, наведений у таблиці 1, демонструє, що вдосконалений метод генерації контейнерів за допомогою ШІ забезпечує кращі показники якості. Це підтверджує ефективність використання адаптивних стеганоносіїв для мінімізації візуальних спотворень та успішного приховування інформації.

Для демонстрації результатів роботи проведено експериментальне порівняння зображень, отриманих за допомогою реалізованого алгоритму із застосуванням оптимізованих промптів, та звичайних генерацій без додаткових інструкцій і ШІ-коригування.

Для проведення експерименту було обрано тематику «balls». В першому випадку, під час генерації використано розширений промпт, у якому вказано всі необхідні параметри для формування носія, що максимально відповідає критеріям якісного стеганоконтейнера. Результати генерації наведено на рис. 6а та рис. 6б.



а) б)

Рис. 6. Генерація стеганоконтейнера із заданим промптом для ШІ

Далі вбудуємо в ці зображення повідомлення «Thisismysecretmessage», використовуючи метод Коха-Жао та проаналізуємо результат (рис. 7а та рис. 7б).

а) б)

Рис. 7. Згенеровані стеганоконтейнери із вбудованим повідомленням

Як показують результати наведені на рис. 7а та рис. 7б, у сформованих стеганосистемах ознаки присутності прихованого повідомлення практично відсутні, за виключенням мінімальних візуальних артефактів.

Традиційно структурні спотворення, що виникають внаслідок застосування стеганографічних методів у просторовій або частотній областях, характеризуються низьким рівнем помітності для людського ока. Більшість сучасних стеганоалгоритмів орієнтовані на забезпечення високої візуальної скритності модифікацій, що було успішно досягнуто в межах запропонованого вдосконаленого методу. Необхідно також враховувати, що ступінь візуалізації деструктивних змін суттєво залежить від обраного методу вбудовування та параметрів стеганоалгоритму, проте ключовим фактором залишаються апріорна якість і морфологічні характеристики самого зображення-носія.

Для подальшого порівняння, наступним кроком, за аналогічним запитом «balls» оберемо два випадкові зображення (без попередньої оптимізації параметрів). Результати наведені на рис. 8а та 8б.

Наступним кроком вбудуємо в ці зображення повідомлення «Thisismysecretmessage», використовуючи метод Коха-Жао та проаналізуємо результат (рис. 9а та рис. 9б).

При порівнянні рис. 8 та рис. 9 можна виділити зображення, яке успішно пройшло етап вбудовування і не виявляє видимих ознак модифікації (рис. 9б). Водночас на рис. 9а чітко помітні дефекти, спричинені внесенням даних. У разі автоматичної генерації контейнерів без попереднього налаштування параметрів або контролю результату, зловмисник легко виявить наявність сторонніх перетворень. Отже, подібні типи носіїв є нестійкими до стеганоаналізу та непридатними для надійного захисту інформації.

а) б)

Рис. 8. Стеганоконтейнери за запитом «balls»без додаткових вказівок

а) б)

Рис. 9. Згенеровані стеганоконтейнери із вбудованим повідомленням

Ефективність згенерованих контейнерів та відсутність на них видимих ознак вбудовування пояснюється врахуванням характеристик зорової системи людини під час вдосконалення методу. При порівнянні очевидно, що синтезовані зображення мають спокійнішу кольорову гаму порівняно з довільно обраними аналогами. У згенерованих носіях відсутні надмірна контрастність та яскраві акценти, які чітко простежуються у другій категорії зображень. Також можна зробити висновок, що використання «простих» візуальних форм (плавних ліній та закруглень) призводить до значно меншої кількості артефактів порівняно зі складними геометричними структурами.

Отже, отримані результати підтверджують успішну реалізацію вдосконаленого методу генерації стеганографічних контейнерів на основі системи штучного інтелекту Midjourney.

Висновки

У роботі розглянуто підхід до підвищення безпеки прихованої передачі даних шляхом удосконалення процесу формування стеганоконтейнерів. Проведений аналіз показав, що використання готових статичних зображень як носіїв створює додаткові ризики, оскільки вбудовування інформації змінює їхні природні статистичні характеристики, що може бути виявлено сучасними методами пасивного стеганоаналізу.

Для вдосконалення формування стеганоконтейнерів доцільно використовувати нейромережу. Запропоновано підхід, який передбачає генерацію контейнера безпосередньо під параметри секретного повідомлення із застосуванням системи штучного інтелекту Midjourney, яка синтезує унікальні зображення на основі текстових запитів (промптів).

Головною перевагою такого підходу є можливість врахувати властивості зорової системи людини ще на етапі створення носія, що робить його візуально стійкішим до виявлення змін порівняно з готовими фото. Процес керується шляхом сегментації промпту на маркери, які система інтерпретує для побудови графічного об'єкта, тому аналітичне складання тексту запиту є визначальним фактором для отримання якісного та стійкого до стеганоаналізу контейнера.

Синтез зображень із заданими структурними та текстурними властивостями дозволяє сформувати носій, більш придатний для вбудовування даних у частотній області. На відміну від традиційної схеми, де модифікується вже наявне зображення, запропонований підхід переносить акцент на етап контрольованого створення контейнера.

Результати порівняльного аналізу свідчать про підвищення стійкості до статистичного виявлення та зменшення рівня візуальних спотворень порівняно з використанням типових зображень-носіїв. Виходячи із даних, що отримані після проведення експериментального дослідження, застосування інтелектуально згенерованих контейнерів забезпечує:

– зменшення середньої абсолютної різниці пікселів на 16 %;
– зниження нормованої абсолютної похибки на 17,6 %;
– зменшення локальної середньоквадратичної помилки (LMSE) у 4 рази (75 %);
– підвищення показника структурної подібності IF до 0,99985;
– зростання нормованої взаємної кореляції на 0,33 %;
– підвищення сигма-відношення сигнал/шум (SSNR) на 4,9 %;
– покращення узагальненого показника GSSNR на 5 %;

– зменшення статистичних відхилень гістограм приблизно на 5,8 %.

Отримані результати свідчать, що попередній синтез стеганоконтейнера дозволяє суттєво мінімізувати візуальні та статистичні аномалії, що виникають під час вбудовування інформації, та підвищує стійкість стеганосистеми до пасивного стеганоаналізу.

Головна відмінність запропонованого підходу полягає у переході від пасивного вибору готового зображення до його цілеспрямованого синтезу із заданими властивостями. На відміну від традиційних методів, які використовують статичні бази цифрових фото, застосування штучного інтелекту дозволяє адаптувати структуру носія під конкретний обсяг даних, забезпечуючи відсутність різких контрастів та складних акцентів ще на етапі створення.

Такий підхід гарантує унікальність кожного контейнера, що унеможливлює порівняння з оригіналом, та дозволяє маскувати внесені зміни під природні шуми ШІ-генерації, значно підвищуючи стійкість до засобів стеганоаналізу.

Таким чином, запропоноване дослідження спрямоване на підвищення ефективності стеганографічного приховування інформації шляхом зміни традиційного підходу до формування контейнера. Підхід, що реалізовано у роботі, дозволяє формувати зображення з керованими текстурними та статистичними характеристиками, що забезпечують краще маскування змін, внесених під час вбудовування даних у DCT-області методом Коха-Жао. У результаті контейнер розглядається не як пасивний носій інформації, а як оптимізоване середовище приховування, що підвищує непомітність модифікацій, зменшує рівень спотворень та покращує стійкість стеганосистеми до статистичного аналізу.

Подальші дослідження доцільно спрямувати на оцінювання стійкості синтезованих контейнерів до активних атак, а також на автоматизацію формування запитів до генеративних систем з урахуванням обсягу даних, що вбудовуються у частотну область дискретного косинусного перетворення.

СПИСОК ЛІТЕРАТУРИ

1. Khoroshko V. O., Yaremchuk Y. E., Karpinets V. V. Computer Steganography: A Textbook. Vinnytsia: VNTU, 2017. 155 p.

2. Shvidchenko I. V. Methods for Detecting Steganographic Data Hiding in Images. *Visnyk of the National University "Lviv Polytechnic". Series: Automation, Measurement and Control*. 2012, №41. P. 198–203. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3737/shvidchenkoiv.pdf (дата звернення 20.12.2025).

3. Khoma D. Y. Modification of the steganographic model STEGANOGAN, based on the advanced generative architectures (Ukr). *Scientific Works of Vinnytsia National Technical University*. 2025. №2. URL: https://doi.org/10.31649/2307-5376-2025-2-155-170 (дата звернення 20.12.2025).

4. Vovk O. O., Astrakhantsev A. A. Development of a Methodology for Evaluating the Importance of Steganographic Algorithm Features. *Visnyk of the National University "Lviv Polytechnic". Information Systems and Networks, Lviv*. 2014. №805. P. 52–60.

5. Hornytska D. A., Volianska V. V. Determining Importance Coefficients for Expert Evaluation in Information Security. *Information Protection*. Kyiv, 2012. №1. P. 108–121.

6. Bobok I. I., Kobozeva A. A., Sokalskyi S. M. Improving the Method of Steganographic Container Selection to Increase the Robustness of Stego Systems Against Embedded Message Attacks. *Herald of Higher Educational Institutions. Radioelectronics*. 2025. URL: https://doi.org/10.20535/S0021347025030045 (дата звернення 20.12.2025)

7. Enhancing the robustness of digital watermarking to attacks based on adaptive coefficient ion in the frequency domain of an image / Y. Yaremchuk et al. *Proc. SPIE 14009, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments* 2025. 30 December 2025. 140090Y. URL: https://doi.org/10.1117/12.3099532(дата звернення 20.12.2025)

8. Enhancing the steganographic resistance of hidden information to active attacks / Y. Yaremchuk et al. *Proceedings of the International Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024)*, Kyiv. October 26, 2024. Vol. 3826. P. 350–355.

9. Midjourney: official website. URL: https://www.midjourney.com/ (дата звернення 20.12.2025).

10. Hrytsiuk V. K., Zolotaryov V. A. Comparison of the Robustness of Koch–Jao and DWT Steganographic Methods Against Various Types of Distortions by Software Tools. *Information Processing Systems*. 2020.№1(160). P. 136–144. URL: https://doi.org/10.30748/soi.2020.160.18 (дата звернення 20.12.2025).

11. Kovtun V., Hnatyuk S., Kinzeriavyi O. Systematization of Modern Computer Steganography Methods. *Information Security*. 2013. Vol. 19, №3. P. 209–217. URL: https://doi.org/10.31649/2307-5376-2025-2-155-170 (дата

звернення 20.12.2025).

Стаття надійшла до редакції 28.02.2026.
Стаття пройшла рецензування 06.03.2026.
Стаття опублікована 31.03.2026.

Карпінець Василь Васильович – канд. техн. наук, доц. кафедри Менеджменту та інформаційної безпеки, ORCID: 0000-0001-8148-2002, e-mail: karpinets@vntu.edu.ua.

Присяжний Дмитро Петрович – асистент кафедри Менеджменту та інформаційної безпеки, ORCID: 0009-0000-8327-3183.

Безпалий Кирило Валерійович – асистент кафедри Менеджменту та інформаційної безпеки, ORCID: 0009-0008-0331-9312.

Білоус Віталій Михайлович – асистент кафедри Менеджменту та інформаційної безпеки, ORCID: 0009-0001-2350-1583.

Тельнік Дмитро Володимирович – магістр кафедри Менеджменту та інформаційної безпеки, ORCID: 0009-0002-2636-8877.
Вінницький національний технічний університет.