УДК 004.056.55; 004.9; 003.26.

І. Д. Казміді[1], В. Ю. Зубок[1,2]
[1]Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Проспект Берестейський, 37, 03056 Київ, Україна
email: ivkaz-ipt22@lll.kpi.ua
[2]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
вул. Олега Мудрака 15, Київ, Україна
email: vitalii.zubok@pimee.ua

Підходи до оптимізації швидкодії зчитування стеганографічної інформації у векторних зображеннях

Розглянуто проблему низької швидкодії процесу зчитування стеганографічної інформації з векторних зображень, зокрема в контексті використання CAD-документації (*цифрових проєктних файлів, що подають об'єкти як математично визначені геометричні елементи на основі векторної графіки) у системах інформаційної безпеки. Показано, що за відсутності апріорної інформації про розміщення прихованих даних вилучення стеганографічної інформації зводиться до повного перебору графічних об'єктів, що призводить до значних обчислювальних витрат і обмежує практичну застосовність відповідних методів. Проведено декомпозицію процесу зчитування на окремі етапи та проаналізовано фактори, які найбільше впливають на його продуктивність. На основі сценарного аналізу витоку інженерних даних сформульовано постановку задачі оптимізації процесу вилучення стеганографічної інформації. Обґрунтовано можливі напрями зменшення обчислювальної складності зчитування без зниження стійкості, ємності та непомітності стеганографічних алгоритмів.*

Ключові слова: *стеганографія, векторні зображення, цифрові водяні знаки, CAD-дані, швидкодія алгоритмів; зчитування прихованої інформації; інформаційна безпека; обчислювальна складність.*

Вступ

Стеганографія у векторних зображеннях на сьогодні розглядається як один із перспективних інструментів захисту інформації, зокрема в контексті охорони авторських прав, протидії витокам даних і забезпечення відслідковуваності цифрових об'єктів [1–3]. Значна частина сучасних досліджень зосереджена на розробці мето-

дів вбудовування прихованої інформації у геометричні параметри векторних об'єктів, таких як координати вершин, параметри кривих або топологічні характеристики, а також на підвищенні їхньої стійкості до активних атак, зокрема афінних перетворень, редагування структури зображення чи зміни форматів файлів [4–6]. Окрему увагу приділяють збереженню візуальної і геометричної якості контейнера, що є критично важливим для інженерних і геоінформаційних застосувань, де навіть незначні спотворення можуть бути неприйнятними [7].

У практичних сценаріях використання, зокрема при роботі із CAD-схемами та іншими складними векторними зображеннями, дедалі більшої ваги набуває питання швидкодії стеганографічних алгоритмів. Такі документи можуть містити тисячі або десятки тисяч геометричних примітивів, при цьому вбудована інформація часто розподіляється між кількома об'єктами з метою підвищення стійкості та непомітності [8, 9]. За відсутності інформації про місце вбудовування процес пошуку та зчитування водяного знаку зводиться до послідовного аналізу всіх елементів зображення, що призводить до значних обчислювальних витрат. У роботах, присвячених захисту CAD-даних, зазначається, що саме етап вилучення водяного знаку часто є вузьким місцем з точки зору продуктивності, особливо після застосування форматних перетворень або редагування даних [10–12]. Попри очевидну практичну значущість, аспект швидкодії здебільшого залишається другорядним у наукових публікаціях, поступаючись увазі питанням стійкості та непомітності [2, 6]. Такий дисбаланс ускладнює впровадження стеганографічних методів у системах інформаційної безпеки, де важливими є не лише факт наявності водяного знаку, а й можливість його оперативного виявлення та зчитування у стислі часові рамки, що є критичним, зокрема, для задач розслідування витоків інформації [11, 13].

Процес накладання цифрових водяних знаків на векторні CAD-схеми є окремим напрямом досліджень у сфері захисту інженерних даних та авторських прав. У наукових роботах розглядаються як видимі, так і невидимі (сліпі або напівкрихкі) водяні знаки, які вбудовуються безпосередньо в геометричну структуру креслень для ідентифікації автора та відстеження походження файлів [14]. Зокрема, для двовимірної інженерної графіки запропоновано реверсивні схеми водяних знаків, що дозволяють повністю відновити оригінальне креслення після автентифікації, використовуючи модифікації координат вершин або методи зсуву гістограм [15, 16]. Такі підходи демонструють можливість збереження високої точності CAD-схем за умови достатньої стійкості до базових геометричних операцій, однак водночас підкреслюють, що продуктивність процедур вбудовування та вилучення є критичним фактором ефективності, оскільки складна структура CAD-даних суттєво відрізняється від растрових зображень і вимагає спеціалізованих алгоритмів обробки [17].

Метою цієї роботи є аналіз проблеми швидкодії вилучення стеганографічної інформації з векторних зображень і систематизація можливих підходів до її оптимізації без зниження рівня захищеності.

У зв'язку з цим постає необхідність комплексного аналізу обчислювальної складності стеганографічних алгоритмів для векторних зображень і розробки підходів, спрямованих на оптимізацію процесів детектування та вилучення прихованої інформації без зниження рівня захищеності.

Постановка задачі та методологія дослідження

Проблема низької швидкодії зчитування стеганографічної інформації з векторних зображень зумовлена необхідністю повного перебору графіч-них об’єктів і виконання для кожного з них обчислювально затратних операцій зчитування та перевірки валідності за відсутності інформації про місце вбудовування даних. У цих умовах час вилучення прихованої інформації зростає пропорційно кількості об’єктів зображення та складності використовуваного стеганографічного алгоритму, що обмежує практичну застосовність таких методів у системах інформаційної безпеки. У зв’язку з цим у статті ставиться задача формалізації процесу зчитування стеганографічної інформації з векторних зображень з точки зору його обчислювальної складності та визначення підходів, які дозволяють зменшити кількість операцій повного зчитування шляхом попередньої ідентифікації або відсіву об’єктів, що не містять прихованих даних.

Для виконання поставленої задачі як методологічну основу було обрано комплексний підхід, що поєднує аналіз наукових джерел, структурно-функціональне моделювання та концептуальний аналіз обчислювальної складності стеганографічних алгоритмів для векторних зображень. На першому етапі було проведено систематизований огляд сучасних наукових публікацій, присвячених стеганографії і цифровим водяним знакам у векторних і CAD-зображеннях, з акцентом на методи вбудовування, стійкість до атак і практичні аспекти використання [1–9, 14–17]. Далі виконано декомпозицію процесу зчитування прихованої інформації на окремі етапи, що дозволило проаналізувати вплив кожного з них на загальну швидкодію алгоритму. Для формалізації проблеми було використано сценарний підхід на прикладі інженерного підприємства, яке зазнало витоку даних, що дало змогу пов’язати теоретичні положення з практичними умовами експлуатації систем інформаційної безпеки. Для конкретизації проблематики далі розглядається умовна ситуація на прикладі інженерного підприємства, яке зазнало атаки витоку даних. Для зображення взаємодії об’єктів розглянемо схему.

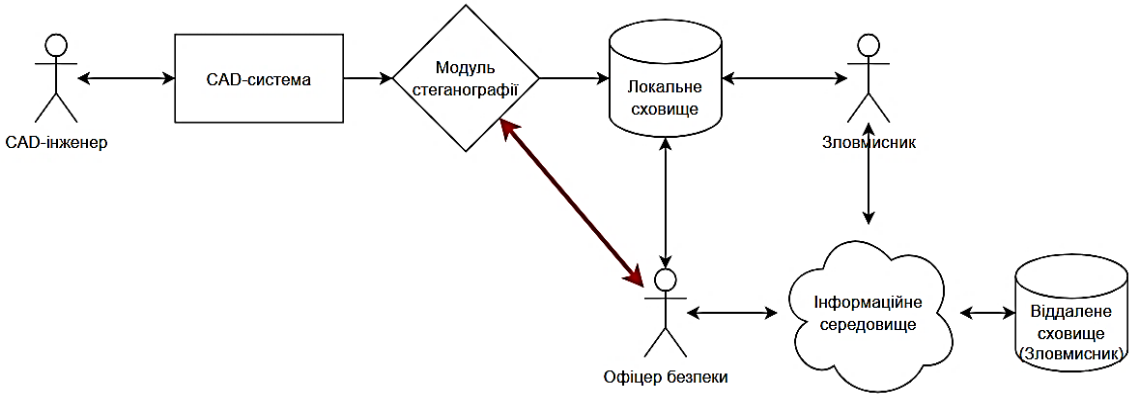

Схема атаки витоку даних інженерного підприємства

На наведеній схемі знаходяться такі об’єкти:

1) CAD-інженер — особа, працівник підприємства, що взаємодіє із CAD-системою та створює інженерні креслення та CAD-схеми;

2) CAD-система — набір програмних засобів, які дозволяють проектувати інженерні креслення, дані яких повністю або частково зберігаються у форматі векторних зображень;

3) модуль стеганографії — програмний засіб, який дозволяє проводити процеси вбудовування та зчитування інформації, занесеної у векторні зображення із використанням методів стеганографії. Модуль автоматично викликається CAD-системою під час файлових операцій над кресленнями для занесення в них прихованої інформації (наприклад, ідентифікатор автора схеми, час зберігання файлу тощо);

4) локальне сховище — інформаційне сховище підприємства, де розміщуються інженерні схеми.

5) зловмисник — особа, яка певним чином отримала санкціонований або несанкціонований доступ до локального сховища та викрала інженерні схеми для злочинного використання;

6) інформаційне середовище — середовище, через яке зловмисник взаємодіє із сторонніми інформаційними системами (наприклад, мережа Інтернет);

7) віддалене сховище (зловмисник) — інформаційне сховище зловмисника, з яким зловмисник взаємодіє через інформаційне середовище з метою зберегти вкрадені інженерні схеми;

8) офіцер безпеки — особа, працівник підприємства, яка відповідальна за інформаційну безпеку підприємства.

Відповідно до зазначеної схеми, послідовність взаємодії об’єктів схеми наступна:

1) CAD-інженер використовує CAD-систему для проектування інженерних схем;

2) CAD-система, під час спроби зберігання інженерної схеми у сховищі, використовує модуль стеганографії для вбудовування прихованої інформації у схему, після чого зберігає файл схеми в локальному сховищі;

3) зловмисник, маючи доступ до локального сховища, копіює інженерну схему і передає її через інформаційне середовище у своє віддалене сховище;

4) офіцер безпеки певним чином дізнається про факт витоку інформації (наприклад, через знахідку відповідної секретної інформації у відкритому доступі в мережі Інтернет). Офіцер безпеки далі взаємодіє з модулем стеганографії та, за потреби, з локальним сховищем з метою зчитування вбудованої в опубліковану схему інформації і подальшого розслідування інциденту та викриття каналу витоку даних підприємства (зловмисника).

Згадана проблема швидкодії на даній схемі виникає під час взаємодії офіцера безпеки та модуля стеганографії, що позначено червоною стрілкою. У випадку наявності великої кількості об’єктів на схемі, модуль стеганографії буде змушений витрачати зайвий час на пошук тих об’єктів, в яких знаходиться вбудована інформація. Враховуючи те, що для перевірки коректності зчитування інформації необхідно провести повний цикл зчитування і перевіряти його результат на предмет наявності зрозумілих даних чи даних в певному очікуваному форматі, відсутність

знань про те, в яких об'єктах вбудована інформація, значно підвищує обчислювальну складність зчитування прихованих даних.

Проблема швидкодії буде погіршуватися у наступних випадках:

— замість однієї схеми відбувається витік кількох схем. У такому випадку витрати на обчислення зростуть відповідно до кількості схем і кількості об'єктів у них;

— зчитування вбудованої інформації відбувається з великою частотою у зв'язку з іншими процесами в підприємстві (наприклад при взаємодії зі сторонніми системами, або під час перевірки знайденої в Інтернеті схеми на предмет дозволу схеми на публікацію);

— стеганографія використовується виключно як метод збереження інформації у векторному зображенні, а цінність становить не лише зображення, але й сама прихована інформація (наприклад при масовому використанні власноручного цифрового підпису [18]);

— стеганографічна інформація перед вбудовуванням у зображення підлягає певним математичним перетворенням (наприклад, шифруванню), і, відповідно, потребує зворотних перетворень при читанні стеганографічної інформації. У такому випадку кожна спроба читання потенційно правильного набору об'єктів буде додатково уповільнена необхідністю розкодувати зчитані дані для перевірки їх на дійсність.

Враховуючи наведені речі, можна конкретизувати, що проблема швидкодії зчитування інформації у зазначених ситуаціях пов'язана з відсутністю можливості заздалегідь знати, в які частини векторного зображення відбулося вбудовування інформації, що, разом із неможливістю проміжної перевірки зчитаних даних на правильність, призводить до витрачення обчислювальних ресурсів і часу на пошук потрібних об'єктів на зображенні. Об'єктом проблеми, в такому випадку, є стеганографічний модуль. Згадана проблема є особливо актуальною для інформаційних систем, в яких постійно виконується зчитування стеганографічної інформації з векторного зображення.

Пропозиції щодо стратегій оптимізації стеганографічного модуля

Керуючись інформацією, отриманою під час наведеного раніше аналізу проблеми, можливо запропонувати наступні методи вирішення зазначеної проблеми швидкодії.

Вбудовування максимальної кількості інформації в окремі об'єкти

Опис ідеї. Інформація вбудовується таким чином, щоб кожен окремий об'єкт векторного зображення містив достатній обсяг прихованих даних, що дозволяє зчитувати кожен об'єкт лише один раз для отримання всієї інформації.

Переваги. Зменшується кількість операцій зчитування даних, оскільки немає потреби багаторазово аналізувати один і той самий об'єкт. Це потенційно підвищує загальну швидкодію стеганографічного модуля.

Недоліки. Існують жорсткі обмеження на обсяг інформації, яку можна приховати в одному об'єкті або його параметрах. Крім того, зберігається необхідність перебору всіх об'єктів зображення для визначення наявності вбудованих даних.

Використання заздалегідь визначених об’єктів-контейнерів

Опис ідеї. До кожного векторного зображення додаються спеціальні об’єкти (наприклад, логотипи), які завжди використовуються як контейнери для прихованої інформації.

Переваги. Спрощується процес пошуку та зчитування прихованих даних, оскільки місце їхнього вбудовування є наперед відомим і не потребує аналізу всього зображення.

Недоліки. Такий підхід порушує базові принципи стеганографії, зокрема секретність факту вбудовування та стійкість до видалення прихованої інформації. У разі розкриття цього механізму зловмисник може легко ідентифікувати та видалити об’єкти-контейнери разом із прихованими даними.

Маркування об’єктів, які містять приховану інформацію

Опис ідеї. Об’єкти, в які вбудовано інформацію, додатково маркуються, що дозволяє швидко ідентифікувати їх перед безпосереднім зчитуванням прихованих даних.

Переваги. Зменшується кількість об’єктів, які необхідно перевіряти повним алгоритмом вилучення інформації. Метод особливо ефективний у випадках, коли дані розподілені між кількома об’єктами, оскільки дозволяє відкинути хибні кандидати на ранньому етапі.

Недоліки. Виникає складність у забезпеченні сумісності алгоритмів маркування та вбудовування інформації. Існує ризик, що маркер може пошкодити приховані дані або навпаки — процес вбудовування знищить маркування.

Вбудовування допоміжної інформації для пошуку основних контейнерів

Опис ідеї. Додатково вбудовується інформація, яка описує розташування або характеристики основних об’єктів-контейнерів, що дозволяє знайти їх без окремого механізму маркування.

Переваги. Дає змогу уникнути проблеми несумісності алгоритмів маркування та основного стеганографічного вбудовування, спрощуючи логіку пошуку контейнерів.

Недоліки. Зростає кількість задіяних об’єктів і складність зображення, а також виникає необхідність застосування кількох стеганографічних методів одночасно. Це призводить до накопичення недоліків кожного з них і зберігає проблему пошуку додаткових об’єктів-контейнерів.

Використання природних особливостей зображення як маркерів

Опис ідеї. Для вбудовування інформації відбираються об’єкти з наперед визначеними спільними характеристиками (наприклад, кілька кіл однакового радіусу), які фактично виконують роль маркерів без додаткового модифікування.

Переваги. Дозволяє відфільтрувати хибні об’єкти ще до етапу зчитування прихованої інформації, зменшуючи обчислювальні витрати. Відсутня необхідність окремого маркування або верифікації шляхом зчитування даних.

Недоліки. Метод накладає жорсткі вимоги на структуру зображення-контейнера. За відсутності необхідної кількості об’єктів або за наявності зайвих схожих об’єктів процес вбудовування та вилучення інформації може стати складним або взагалі неможливим.

Описані вище методи можна занести у спільну таблицю.

Запропоновані вирішення проблеми швидкодії

№	Опис рішення	Переваги	Недоліки
1	Вбудовування максимальної кількості інформації в окремі об’єкти зображення	Зменшується кількість зчитувань, підвищується швидкодія	Обмежений обсяг даних в одному об’єкті, необхідний перебір усіх об’єктів
2	Використання наперед визначених об’єктів-контейнерів	Спрощується пошук і зчитування прихованої інформації	Можливе порушення секретності, дані легко виявити та видалити
3	Маркування об’єктів із прихованою інформацією	Швидкий відбір потрібних об’єктів, зменшення обчислювальних витрат	Складність сумісності маркування та вбудовування даних
4	Вбудовування допоміжної інформації для пошуку контейнерів	Зникає потреба суміщення маркування та вбудовування інформації в один об’єкт	Зростає складність реалізації і кількість стеганографічних методів. Потенційне зменшення стійкості до знищення інформації.
5	Використання природних особливостей зображення як маркерів	Відсіювання хибних об’єктів без зчитування даних	Жорсткі вимоги до структури зображення-контейнера

Висновки

Розглянуто проблему швидкодії зчитування стеганографічної інформації з векторних зображень. Приведено приклад такої проблеми на умовній схемі інженерного підприємства, яке зазнало атаку витоку даних. Сформовано визначення проблеми — низька швидкодія вилучення стеганографічної інформації зумовлена необхідністю пошуку та перебору об’єктів зображення на предмет наявності в них зазначеної прихованої інформації. Окрім того, запропоновано варіанти вирішення проблеми, їхні потенційні переваги та недоліки, які потребують подальшого дослідження, аналізу ефективності оптимізації використання обчислювальних ресурсів і впливу на характеристики стеганографічного алгоритму, зокрема ємність і непомітність.

Вирішення зазначеної проблеми дозволить зменшити витрати на обчислювальні ресурси під час взаємодії з векторними стеганографічними контейнерами, що розширить потенціал використання стеганографії векторних зображень.

1. Katzenbeisser S., Petitcolas F. A. P. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

2. Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. *Digital Watermarking and Steganography*. 2nd ed., Morgan Kaufmann, 2008.

3. Petitcolas F. A. P., Anderson R. J., Kuhn M. G. Information hiding — a survey. *Proceedings of the IEEE*, 1999, Vol. 87(7), pp. 1062–1078.

4. Ohbuchi R., Ueda H., Endoh S. Robust watermarking of vector digital maps. *Proc. IEEE International Conference on Multimedia and Expo*, 2002.

5. Wang Y., Men C., Wang J. A blind watermarking scheme for vector geospatial data. *Computers, Environment and Urban Systems*, 2010.

6. Kinzeriavyi O. M. *Steganographic methods of data hiding in vector images resistant to active attacks based on affine transformations*. PhD Thesis, 2019.

7. Voigt M., Busch C. Watermarking of CAD drawings for copyright protection. *Proceedings of SPIE*, 2005.

8. Hou Y., Li S. Watermarking for vector graphics based on geometric invariants. *Journal of Visual Communication and Image Representation*, 2007.

9. Peng F., Li X., Yang B. Adaptive watermarking for vector graphics. *IEEE Transactions on Multimedia*, 2014.

10. Zhao H., Koch E. Embedding robust labels into vector data for map copyright protection. *Proceedings of ACM Multimedia*, 2000.

11. Liu R., Tan T. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 2002.

12. Wu M., Liu B. Data hiding in digital vector maps. *IEEE Signal Processing Magazine*, 2003.

13. Katzenbeisser S., Petitcolas F. A. P. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

14. Wu J., Zhou J., Li Q. A robust watermarking algorithm for 2D CAD engineering graphics. *Lecture Notes in Computer Science*, Springer, 2013.

15. Peng F., Long M., Li X. Reversible watermarking for 2D CAD engineering graphics based on improved difference expansion. *Computer-Aided Design*, 2011.

16. Peng F., Li X., Yang B. Reversible watermarking for 2D CAD engineering graphics based on histogram shifting. *Multimedia Tools and Applications*, 2017.

17. Peng F., Li X., Yang B. Performance analysis of watermarking algorithms for CAD data. *Multimedia Systems*, 2018.

18. Про затвердження Положення про застосування цифрового власноручного підпису в банківській системі України: Постанова Національного банку України від 13.12.2019 № 151. База даних «Законодавство України» / Верховна Рада України.

Надійшла до редакції 12.02.2026