УДК: 004.056.5

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЕКТОРНИХ ЗОБРАЖЕНЬ ВІД АТАК СПРЯМОВАНИХ НА ВИДАЛЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

Карпінець В. В., Яремчук Ю.Є.

ANALYSIS OF POSSIBLE ATTACKS ON VECTOR IMAGES AIMED AT REMOVING DIGITAL WATERMARKS

Karpinets V., Yaremchuk Yu.

У роботі розглянуто особливості можливих атак на векторні зображення, спрямованих на зчитування, видалення чи підміну цифрових водяних знаків (ЦВЗ), і встановлено, що найбільш важливим для стеганографічних методів, що витягують ЦВЗ без необхідності оригіналу зображення чи самого ЦВЗ, є забезпечення стійкості до активних зловмисних атак, спрямованих на ускладнення витягування ЦВЗ правовласником.

Також проведено аналіз методів оцінювання впливу зловмисних атак на векторні зображення. Результати аналізу показали, що досить ефективними є методи, які за допомогою показників якості, відмінності та кореляційних показників визначають відмінність між оригіналом зображення та зміненим внаслідок проведених атак та вбудовування ЦВЗ.

Ключові слова: *стеганографія, цифровий водяний знак, захист авторського права, векторні зображення.*

Вступ

Сьогодні задача захисту цифрової інформації є дуже актуальною з урахуванням стрімкого розвитку інформаційних технологій. Зокрема, особливої уваги все більше потребує захист авторського права цифрових даних. Для цього широко використовують стеганографічні методи вбудовування цифрових водяних знаків у мультимедійну інформацію, наприклад у цифрові зображення [1]. На даний час запропоновано достатньо велика кількість методів для захисту растрових зображень [1], чого не можна сказати про векторні зображення, які також широко використовуються в інформаційних системах.

Аналіз існуючих методів вбудовування ЦВЗ у векторні зображення показав, шо вони перебувають на етапі розвитку і ще не досягли такого рівня якості та стійкості як методи для растрових зображень [2-4]. В основному, це зумовлено іншим форматом векторних зображень, наприклад, значно меншою надлишковістю векторних даних і, як наслідок, складністю досягнення компромісу між достатньою стійкістю методу та забезпеченням збереження якості зображення. Тому актуальним залишається розробка методів вбудовування ЦВЗ у векторні зображення, які б забезпечували достатній рівень стійкості ЦВЗ до сторонніх атак і при цьому мінімально впливали на якість зображення.

Особливий інтерес викликають методи, які дозволяють витягувати ЦВЗ без необхідності наявності оригіналу зображення, самого ЦВЗ чи іншої додаткової інформації окрім секретного ключа, що також ускладнює задачу забезпечення високої якості та стійкості методу.

Створення й експлуатація надійного стеганографічного засобу передбачає наявність певного інструментарію для його контролю оцінювання. Кількісне оцінювання стійкості стеганографічної системи захисту до зовнішніх впливів являє собою складну задачу, яка зазвичай на практиці реалізується методами системного аналізу, математичного моделювання або експериментального дослідження.

Як правило, стегосистема забезпечує трирівневу модель захисту інформації, що вирішує дві основні задачі [1]. По-перше, це приховування самого факту наявності інформації, що захищається, (перший рівень захисту). По-друге, блокування несанкціонованого доступу до інформації, яке здійснюється шляхом вибору відповідного методу приховування інформації (другий рівень захисту). І нарешті, передбачається третій рівень захисту – криптографічний захист (шифрування) приховуваної інформації.

Структура процесу моделювання та оцінювання стійкості стегосистеми може бути представлена у вигляді [1], як показано на рис. 1. Як видно з наведеної структури, надійність і час стійкості стегосистеми під час проведення аналізу та випробувань визначаються обчислювальними можливостями комплексу. Оцінювання якості основної характеристики стегосистеми – рівня скритності – забезпечується шляхом проведення аналітичних досліджень (стеганоаналізу) і натурних випробувань. Для оцінювання якості стеганографічного приховування часто застосовують відомі методи з інших галузей, у першу чергу – криптоаналізу. Оскільки абонент-одержувач може відновлювати приховану інформацію з прийнятого повідомлення, то існує деякий механізм її витягування.

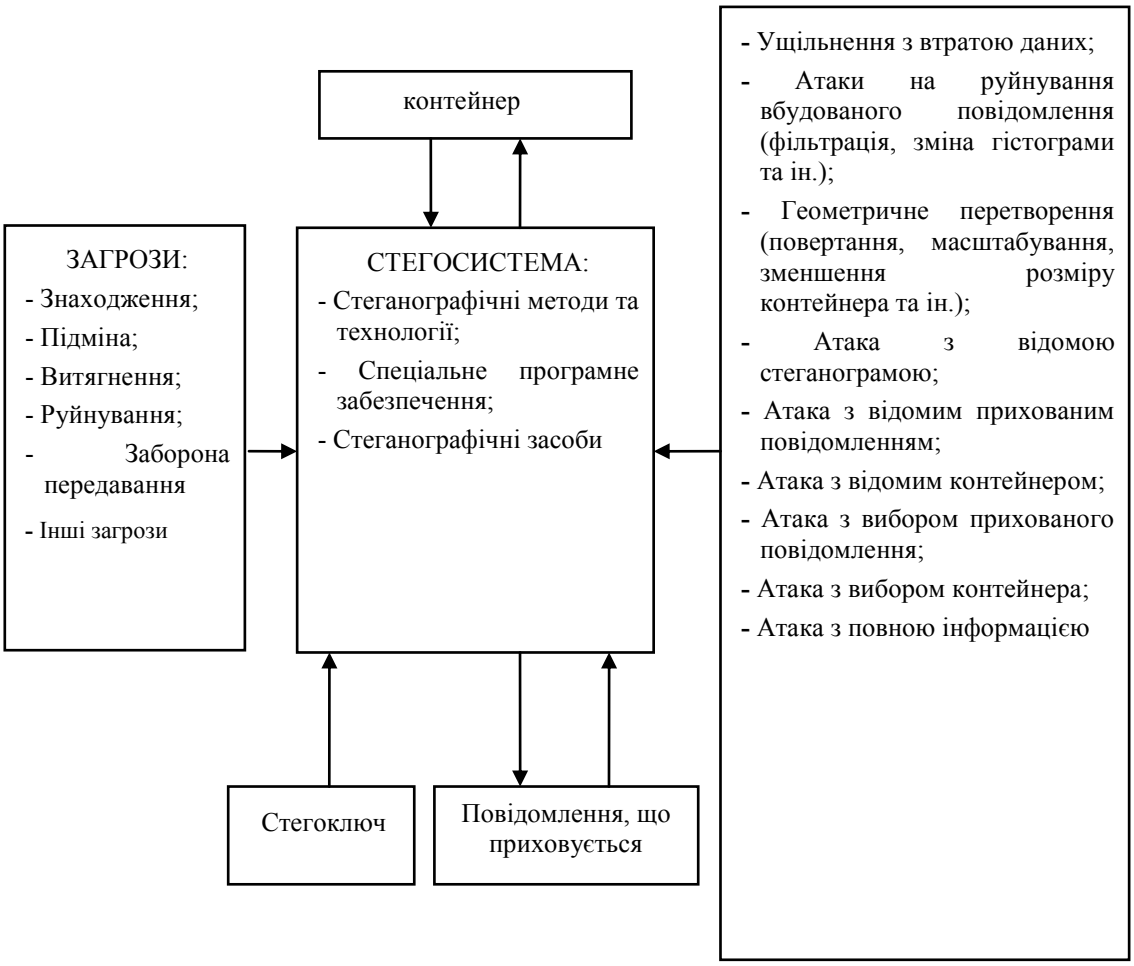

Рис. 1. Модель аналізу загроз і оцінювання стійкості стегосистеми

Якщо зловмисник, висуваючи гіпотези про можливе стеганографічне перетворення, має деякий інструмент для їхньої перевірки, то він має шанси на підтвердження факту існування прихованої інформації, здійснення пошуку механізму витягання секретного повідомлення і розкриття змісту листування. Тому, у першу чергу, як детектування стеганограм можна застосовувати різновиди описаних вище атак на стегосистему і велику частину методів криптоаналізу.

Таким чином, для забезпечення захисту векторних зображень від навмисних спотворень актуальним є дослідження можливих атак, спрямованих на спотворення чи видалення ЦВЗ, а також методів оцінювання рівня спотворення зображення внаслідок їх дії.

Вимоги до ЦВЗ та можливі атаки спотворення векторних зображень

Серед основних вимог до методів вбудовування ЦВЗ [2] слід виділити такі:

- надійність: стійкість векторних зображень з вбудованим ЦВЗ до нападу з використанням різних атак, яка полягає в можливості виявлення і витягнення вбудованого ЦВЗ після атаки;

- непомітність: включає в себе візуальну непомітність змін у графіці і непомітність зміни точності векторних даних після вбудовування ЦВЗ;

- розмір ЦВЗ: кількість інформації, яку вносить ЦВЗ, має забезпечити доведення авторських прав розробника векторних зображень;

- безпека: здатність вбудованого ЦВЗ протистояти незаконним перехопленням і зміні даних.

Однак на практиці вимоги до цих показників є суперечливими. На рис. 2 показані взаємні обмеження і компроміси між стійкістю, непомітністю та розміром ЦВЗ. По-перше, зображення з вбудованим ЦВЗ, як і оригінальне векторне зображення, має бути високої якості. Якщо у векторне зображення вбудовано ЦВЗ малого розміру, то його легше втратити під час обробки векторного зображення. Непомітність вбудованого ЦВЗ стає меншою, коли підвищується стійкість за рахунок збільшення розміру ЦВЗ.

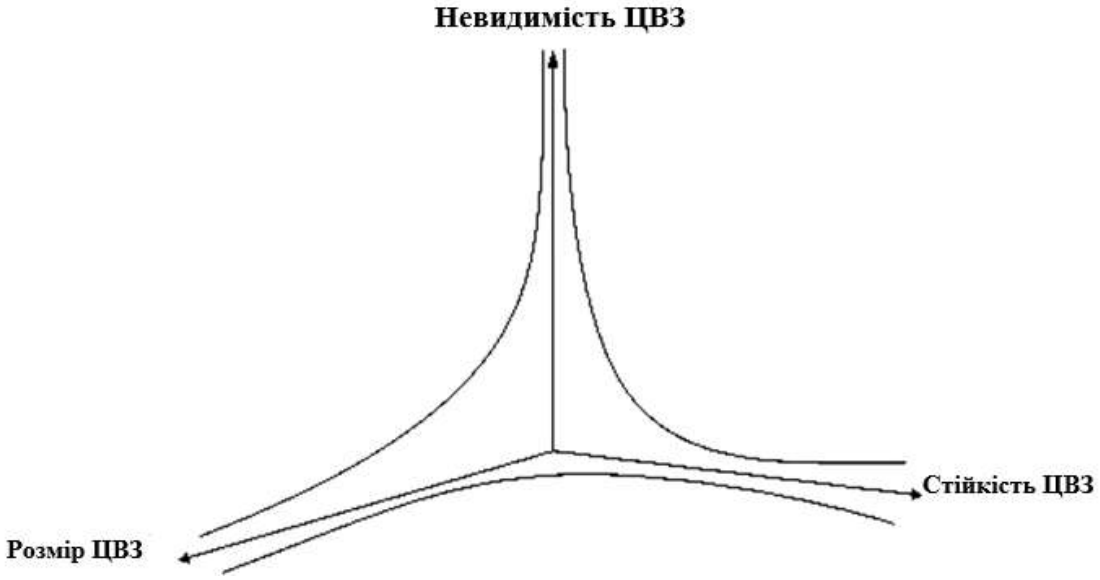

Рис. 2. Взаємні обмеження між стійкістю, непомітністю та розміром ЦВЗ

Аналіз рис. 2 показує, що неможливо одночасно забезпечити максимальну стійкість, непомітність і великий розмір ЦВЗ. На практиці зазвичай можна вибрати компроміс між цими показниками оцінки ЦВЗ.

При оцінюванні стійкості захисту векторних зображень до зловмисних атак слід розглянути фактори, які впливають на стійкість [2].

1. Розмір ЦВЗ.

Важливим параметром є розмір вбудованого ЦВЗ, який безпосередньо пливає на стійкість захисту вбудовування ЦВЗ. При вбудовуванні ЦВЗ більшого розміру, забезпечується вища стійкість.

2. Стійкість (робастність) ЦВЗ.

Стійкість вбудованого ЦВЗ і його непомітність є взаємовиключними. Зі збільшенням стійкості вбудованого ЦВЗ його непомітність зменшується.

3. Місце вбудовування.

Оскільки місце вбудовування може напряму вливати на надійність алгоритму, для вбудовування ЦВЗ обираються нечутливі до втручання області векторного зображення.

4. Розмір і тип векторного зображення.

Незалежно від розміру векторного зображення з вбудованим ЦВЗ стійкі методи вбудовування ЦВЗ мають забезпечувати повне відновлення ЦВЗ у випадку зловмисних атак. Крім розміру зображення, тип зображення також впливає на стійкість ЦВЗ, тому система оцінки стійкості ЦВЗ повинна адаптуватися до якомога ширшого спектра типів і розмірів векторних зображень.

Оцінювання стійкості вбудовування ЦВЗ у векторні зображення зазвичай здійснюється шляхом застосування однієї або декількох атак до векторного зображення з вбудованим ЦВЗ. Потім ЦВЗ витягується з векторного зображення, що було піддано атаці. Після отримання даних про правильність розпізнавання бітів ЦВЗ можна визначати стійкість методу вбудовування ЦВЗ.

Взагалі розрізняють пасивні атаки, що спрямовані на визначення місця розташування та зчитування ЦВЗ без впливу на зображення, та активні, що проводяться з метою пошкодження чи видалення ЦВЗ. Саме активні атаки потребують більшої уваги, оскільки вони спрямовані на порушення авторських прав.

Розглянемо можливі типи активних атак на векторні зображення з вбудованими ЦВЗ.

Атаки, спрямовані на видалення ЦВЗ. Під час проведення атаки, спрямованої на видалення ЦВЗ проводять аналіз векторного зображення, оцінюють інформацію, яку містить ЦВЗ, потім виділяють вбудований ЦВЗ і оригінальне векторне зображення і намагаються повністю видалити інформацію ЦВЗ від векторного зображення, не знаючи конкретних алгоритмів і ключів, які застосовувались для вбудовування ЦВЗ.

Атаки ущільненням векторного зображення. При здійсненні атак такого типу видаляються деякі надлишкові дані, тим самим зменшується розмір векторного зображення з вбудованим ЦВЗ. Головною метою такої атаки є зміщення центральної осі векторних лінійних елементів даних.

Атака ущільнення точок інтервалу. Зберігаючи першу та останню точки кривої, вибирається точка для кожної з N точок з послідовності координат, яка утворюється з вершин прямокутних елементів або лінійних елементів.

Атака ущільнення кута відхилення або атака вертикальної відстані. Для проведення атаки

спочатку обчислюється відстань або кут між поточною точкою і попередньою, потім ця відстань або кут порівнюються з допустимою відстанню по вертикалі або з допустимим кутом відхилення, якщо параметр відповідає або перевершує допустиме значення, точка залишається.

Атака послідовності передачі даних. Мета цієї атаки полягає у впливі на метод витягування ЦВЗ шляхом зміни відносного положення послідовності координат. Оскільки організація точок, ліній і багатокутників відрізняється, то атака послідовності передачі даних також видозмінюється. Така атака реорганізує послідовність координат таким чином, що утворюється одна випадкова послідовність, довжина якої дорівнює загальній кількості вершин, номери яких інколи інвертуються, і відповідно порядок координат в послідовності.

Атака перетворення формату даних. Атака перетворення формату даних переводить векторні дані ГІС з одного формату в інший, а потім перетворює дані з оригінальним форматом, інвертуючи їх.

Атака синхронізації. Мета атаки синхронізації полягає не в тому, щоб повністю видалити інформацію про водяний знак, а в створенні нової векторної карти з непомітними спотвореннями. Це досягається різними геометричними перетвореннями над цією векторною картою. Таким чином порушується синхронізація між методом витягування ЦВЗ та самим ЦВЗ. В результаті здійснених змін метод витягування ЦВЗ не може правильно розпізнати ЦВЗ.

Геометричні атаки змінюють векторні карти, в яких значення координат трохи змінені шляхом трансформації карти із застосуванням невеликих геометричних перетворень. Геометричні атаки включають атаки переміщення, атаки масштабування, атаки повороту, атаки віддзеркалення, афінні атаки, атаки зсуву. Атака переміщення полягає у переміщенні карти на певні відстані по осях координат X, Y; атаки масштабування збільшують або зменшують карту з масштабуванням у кілька разів, при цьому вибирається одна точка – центр масштабування; атаки обертання повертають карту на певний кут, при цій атаці також обирається одна точка як центр обертання; атаки віддзеркалення також називаються симетричними атаками, вони полягають в застосуванні до карти осьового або центрального перетворення симетрії, при цьому вибирається одна лінія в якості осі симетрії, або точка в якості центра симетрії; афінні атаки отримують нові значення координат, переміщуючи, масштабуючи, обертаючи карту чи виконуючи інші складні трансформації.

Атака внесення додаткового шуму. Атака внесення шуму генерує випадкову послідовність шуму, яка має рівномірний розподіл на інтервалі $[a, b]$, і довжина цієї послідовності шуму дорівнює числу точок, які будуть атаковані шляхом додавання шуму, потім відтворюється послідовність положень точки, чия довжина дорівнює довжині послідовності шуму і чиї значення коливаються в межах від одного до загальної кількості вершин, а також відрізняються один від одного. Потім цей шум додається до значень координати точок.

Атаки редагування даних. Атаки редагування даних змінюють векторні карти, вставляючи певний відсоток точок, видаляючи певний відсоток точок або змінюючи координати певного відсотка випадкових точок. Це призводить до переміщення, видалення або зміни деяких вершин багатокутників і зрештою впливає на процес витягнення водяних знаків. Атаки редагування векторних даних ГІС можна розділити на: атаки зміни точок, атаки додавання точок, атаки видалення точок.

Атака відсікання зображення. Атака відсікання зображення базується на обрізці певного відсотка масиву даних у декількох місцях, які спричиняють зникнення деякої частини точок оригінальних даних. Це може спричинити неможливість коректного витягнення інформації водяного знаку у регіоні, в якому відбулася обрізка і, як наслідок, коректного витягнення ЦВЗ.

Атаки проекційного перетворення. Атаки проекційного перетворення полягають в переміщенні векторних даних геоінформаційних систем (ГІС) з однієї проекційної площини до іншої, і подальшого конвертування оригінальних даних ГІС шляхом перетворення інверсії.

Атаки копіювання. Основна ідея атаки копіювання: витягнути оригінальний ЦВЗ, що міститься у векторному зображенні, а потім маркувати ним інші векторні зображення, що його не мають.

Розглянувши особливості можливих атак на векторні зображення, спрямованих на зчитування, видалення чи підміну ЦВЗ, можна сказати, що одними з найважливіших є активні зловмисні атаки, спрямовані на ускладнення витягування ЦВЗ.

Після проведеної атаки потрібно оцінити її вплив на стійкість ЦВЗ. Окрім того, що можна провести витягування самого ЦВЗ і порівняти його з еталоном, важливим і більш інформативним при моделюванні захисту є оцінювання впливу атак саме на зображення з вбудованим ЦВЗ. Це дає змогу не тільки визначити правильність розпізнавання бітів ЦВЗ, а й визначити слабкі місця методу на основі аналізу зображення.

Для оцінювання рівня спотворень внаслідок активних атак на зображення необхідно визначити методи, за якими буде проводитись оцінювання.

Оцінювання рівня спотворень векторних зображень внаслідок проведених атак та вбудовування ЦВЗ

У деяких випадках досить ефективним є метод оцінювання рівня скритності стегозасобів на основі аналізу їхніх статистичних характеристик. Статистична теорія дає кількісні критерії випадковості, що дозволяє створювати «детектори», які виявляють статистичні розбіжності між послідовностями. Якщо є необхідний об'єм аналізованої послідовності, то з досить високою ймовірністю можна судити про випадковості виділеної для аналізу послідовності з контейнера. На початковому етапі аналізу можна скористатися традиційними статистичними (хі-квадрат, тести на заборонені символи, на довжину циклу, «дні народжень»), емпіричними (перевірки частот, серій, інтервалів, перестановок, перевірки на монотонність, покер-тестом, тестом збирача купонів) або спектральними тестами. Далі використовуються більш «тонкі» методи, іноді розроблювані під конкретну задачу.

Для порівняльного оцінювання якості стеганографічних засобів розробляють різні метрики, що дають кількісні оцінки. Найбільша їхня кількість розроблена для стеганометодів (методів цифрових водяних знаків), які працюють із зображеннями. Звичайно такі метрики оперують із зображенням на рівні пікселів, хоча після деякої адаптації вони застосовні і до інших способів опису зображення, а також до аудіоданих. Найбільш популярною метрикою під час аналізу рівня перекручувань, що вносяться у контейнер під час приховування в ньому інформації, є взяте з радіотехніки співвідношення сигнал – шум, яке обчислюється в децибелах [1].

Для оцінювання стійкості захисту ЦВЗ до зловмисних атак пропонується проводити аналіз з точки зору спотворень, які вносить стороннє стеганоперетворення в зображення. Наприклад, для оцінювання стійкості вбудовування ЦВЗ у растрові зображення використовуються критерії якості. Більшість критеріїв якості, які використовуються при візуальній обробці, відносять до групи показників відмінності [3]. Ці показники базуються на відмінності між контейнером-оригіналом і контейнером-результатом. До іншої групи відносяться показники, що базуються на кореляції між оригінальним зображенням і зображенням з вбудованим ЦВЗ (кореляційні показники).

Оскільки усі ці показники показують відмінність між значеннями кольорів пікселів растрового зображення, виходячи з особливостей форматів растрових та векторних зображень, очевидно, що їх можна використати і для векторних зображень, лише за основу взявши не колір пікселів, а координати точок векторного зображення.

Для оцінювання стеганографічних методів можна використати такі показники [1]:

1. Максимальна відмінність (Maximum Difference):

$$MD = \max_{x,y} | C_{x,y} - S_{x,y} | . \quad (1)$$

2. Середня абсолютна відмінність (Average Absolute Difference):

$$AD = \frac{1}{XY} \cdot \sum_{x,y} | C_{x,y} - S_{x,y} | . \quad (2)$$

3. Нормована середня абсолютна відмінність (Normalized Average Absolute Difference):

$$NAD = \sum_{x,y} | C_{x,y} - S_{x,y} | \Big/ \sum_{x,y} | C_{x,y} | . \quad (3)$$

4. Середньоквадратична помилка (Mean Square Error):

$$MSE = \frac{1}{XY} \cdot \sum_{x,y} (C_{x,y} - S_{x,y})^2 . \quad (4)$$

5. Нормована середньоквадратична помилка (Normalized Mean Square Error):

$$NMSE = \sum_{x,y} (C_{x,y} - S_{x,y})^2 \Big/ \sum_{x,y} (C_{x,y})^2 . \quad (5)$$

6. L^p -норма (L^p - norm):

$$L^p = \left(\frac{1}{XY} \cdot \sum_{x,y} | C_{x,y} - S_{x,y} |^p \right)^{\frac{1}{p}} . \quad (6)$$

7. Лапласова середньоквадратична помилка (Laplacian Mean Square Error):

$$LMSE = \sum_{x,y} (\nabla^2 C_{x,y} - \nabla^2 S_{x,y})^2 \Big/ \sum_{x,y} (\nabla^2 C_{x,y})^2 . \quad (7)$$

8. Відношення «сигнал-шум» (Signal to Noise Ratio):

$$SNR = \sum_{x,y} (C_{x,y})^2 \Big/ \sum_{x,y} (C_{x,y} - S_{x,y})^2 . \quad (8)$$

9. Максимальне відношення “сигнал-шум” (Peak Signal to Noise Ratio):

$$PSNR = XY \cdot \max (C_{x,y})^2 \Big/ \sum_{x,y} (C_{x,y} - S_{x,y})^2 . \quad (9)$$

10. Якість зображення (Image Fidelity):

$$IF = 1 - \sum_{x,y} (C_{x,y} - S_{x,y})^2 \Big/ \sum_{x,y} (C_{x,y})^2 . \quad (10)$$

11. Нормована взаємна кореляція (Normalized Cross-Correlation):

$$NC = \sum_{x,y} C_{x,y} \cdot S_{x,y} \Big/ \sum_{x,y} (C_{x,y})^2 . \quad (11)$$

12. Якість кореляції (Correlation Quality):

$$CQ = \sum_{x,y} C_{x,y} \cdot S_{x,y} \Big/ \sum_{x,y} C_{x,y} . \quad (12)$$

13. Структурний вміст (Structural Content):

$$SC = \sum_{x,y} (C_{x,y})^2 \Big/ \sum_{x,y} (S_{x,y})^2 . \quad (13)$$

14. Загальне сигма-відношення «сигнал-шум» (Global Sigma Signal to Noise):

$$GSSNR = \sum_{b} \sigma_b^{\,2} \Big/ \sum_{x,y} (\sigma_b - \tilde{\sigma}_b)^2 , \quad (14)$$

де

$$\sigma_b = \sqrt{\frac{1}{n} \cdot \sum_{блокb} (C_{x,y})^2 - \left(\frac{1}{n} \cdot \sum_{блокb} C_{x,y} \right)^2} .$$

15. Сигма відношення «сигнал-шум» (Sigma Signal to Noise Ratio):

$$SSNR = \frac{1}{n} \sum_{b} SSNR_b , \quad (15)$$

де $SSNR = 10 \cdot \lg \left[\dfrac{\sigma_b^{\,2}}{(\sigma_b - \tilde{\sigma}_b)^2} \right]$.

При цьому $C_{x,y}$ – значення координат точок векторного зображення (*x,y*), $S_{x,y}$ – відповідні координати точок зміненого внаслідок атак зображення з вбудованим ЦВЗ.

Показники (1) – (10) відносять до показників відмінності, що показують різницю між оригіналом векторного зображення та зміненого внаслідок атак зображення з вбудованим ЦВЗ. За допомогою цих показників можна ефективно визначати вплив вбудованого ЦВЗ та можливих атак на якість зображення і стійкість ЦВЗ.

Кореляційні показники (11) – (12) забезпечують оцінювання рівня кореляції між сусідніми точками векторного зображення внаслідок проведених атак та вбудовування ЦВЗ. Такі показники дуже важливі для оцінювання методу вбудовування ЦВЗ з точки зору його стійкості до статистичного аналізу, спрямованого на визначення місця розташування ЦВЗ з боку зловмисника.

Показники (13) – (15) дозволяють глибше оцінити рівень шуму, що вноситься у векторне зображення внаслідок вбудовування ЦВЗ та проведених атак.

Отже усі ці показники дозволять в повній мірі оцінити вплив активних сторонніх атак на векторні зображення з вбудованим ЦВЗ і ти самим визначити рівень стійкості методу до цих атак.

Висновки

Таким чином, проведено дослідження можливості забезпечення стійкість захисту векторних зображень до зловмисних атак. При цьому більшу увагу приділено методам, що витягують ЦВЗ без необхідності оригіналу зображення чи самого ЦВЗ і дозволяють найбільш зручно підтверджувати авторство. Встановлено, що для таких методів захисту векторних зображень найбільш важливим є забезпечення стійкості до активних зловмисних атак, спрямованих на ускладнення витягування ЦВЗ правовласником. Розглянуто особливості можливих активних атак на векторні зображення, спрямованих на зчитування, видалення чи підміну ЦВЗ.

Також було проведено аналіз методів оцінювання впливу зловмисних атак на векторні зображення. Результати аналізу показали, що найбільш ефективними є методи, які за допомогою показників якості, відмінності та кореляційних показників визначають відмінність між оригіналом зображення та зміненим внаслідок проведених атак та вбудовування ЦВЗ.

Література

1. *В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук.* Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ. – 2003. – 143 с.

2. *Liangbin Zheng, Yulu Jia, Qun Wang.* Research on Vector Map Digital Watermarking Technology // First International Workshop on Education Technology and Computer Science – 2009. – P. 303-307. i

3. *Карпінець В. В., Яремчук Ю. Є.* Аналіз впливу цифрових водяних знаків на якість векторних зображень // Сучасний захист інформації. – 2011. – №1. – С.72-82.

4. *Карпінець В. В., Яремчук Ю. Є.* Зменшення відхилень координат точок внаслідок вбудовування цифрових водяних знаків у векторні зображення // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні – 2010. – № 2(21). – С.69-78.

References

1. V.O. Horoshko, O.D. Azarov, M.Є. Shelest, Ju.Є. Jaremchuk. Osnovi komp'juternoї steganografiї. Navchal'nij posibnik. – Vinnicja: VDTU. – 2003. – 143 s.

2. Liangbin Zheng, Yulu Jia, Qun Wang. Research on Vector Map Digital Watermarking Technology // First International Workshop on Education Technology and Computer Science – 2009. – P. 303-307. i

3. Karpinec' V. V., Jaremchuk Ju. Є. Analiz vplivu cifrovih vodjanih znakiv na jakist' vektornih zobrazhen' // Suchasnij zahist informacії. – 2011. – №1. – S.72-82.

4. Karpinec' V. V., Jaremchuk Ju. Є. Zmenshennja vidhilen' koordinat tochok vnaslidok vbudovuvannja

cifrovih vodjanih znakiv u vektorni zobrazhennja // Pravove, normativne, ta metrologichne zabezpechennja sistemi zahistu informacії v Ukraïni – 2010. – № 2(21). – S.69-78.

В. В. Карпинец, Ю. Е. Яремчук

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ВЕКТОРНЫХ ИЗОБРАЖЕНИЙ ОТ АТАК НАПРАВЛЕННЫХ НА УДАЛЕНИЕ ЦИФРОВЫХ ВОДНЫХ ЗНАКОВ

В работе рассмотрены особенности возможных атак на векторные изображения, направленных на считывание, удаление или замену цифровых водяных знаков (ЦВЗ), и установлено, что наиболее важным для стеганографических методов, что извлекают ЦВЗ без необходимости оригинала изображения или самого ЦВЗ, является обеспечение устойчивости к активным вредоносным атакам, направленным на осложнение извлечения ЦВЗ правообладателем.

Также проведен анализ методов оценки влияния вредоносных атак на векторные изображения. Результаты анализа показали, что достаточно эффективны методы, которые с помощью показателей качества, разности и корреляционных показателей определяют различие между оригиналом изображения и измененным вследствие проведенных атак и встраивания ЦВЗ.

Ключевые слова: *стеганография, цифровой водяной знак, защита авторского права, векторные изображения.*

Vasyl Karpinets, Yuriy Yaremchuk

ANALYSIS OF POSSIBLE ATTACKS ON VECTOR IMAGES AIMED AT REMOVING DIGITAL WATERMARKS

The paper deals with features of possible attacks on vector images designed to read, delete or substitute digital watermark, and found that the most important for steganographic techniques that drew digital watermark without the need of the original image or digital watermark is to provide stability to the active malicious attacks aimed at complications pulling digital watermark owner.

It was also analyzed the methods for assessing the impact of malicious attacks on vector images. The analysis showed that there are very effective methods to using quality indicators, differences and correlation parameters determine the difference between the original image and modified as a result of conducted attacks and embedding digital watermark.

Keywords: *steganography, digital watermark, copyright protection, vector image.*

Яремчук Юрій Євгенович - к.т.н., доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету;

Карпінець Василь Васильович - к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.

Рецензент: Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.