УДК: 004.056.5

**В. В. Карпінець;**
**Ю. Є. Яремчук,** канд. техн. наук, доц.

# ДОСЛІДЖЕННЯ СТЕГАНОГРАФІЧНОЇ СТІЙКОСТІ МЕТОДУ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ

*Проведено дослідження стійкості методу вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення, до зловмисних атак, яким можуть бути піддані векторні зображення з вбудованим ЦВЗ. Результати аналізу показали, що метод достатньо стійкий до атак, спрямованих на зчитування, визначення місця розташування, видалення чи підміну ЦВЗ, а також на ускладнення витягування ЦВЗ правовласником шляхом додавання шуму або видалення/додавання точок векторного зображення.*

## Вступ

На сьогодні графічні цифрові зображення векторного формату дуже широко використовуються для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо, на створення яких витрачається багато часу та коштів. В зв'язку з цим актуальною стає задача захисту векторних зображень. При цьому особливий інтерес викликає таке забезпечення захисту, для якого не потрібно наявності оригіналу для підтвердження авторства.

Ця задача вирішується методами вбудовування цифрових водяних знаків (ЦВЗ) у зображення. Серед них найбільшого поширення отримали методи, які базуються на частотних перетвореннях. До таких методів відносяться методи Базіна–Барса–Маделана, Хе–Жу–Ванга, Солачідіса–Ніколаїдіса–Пітаса [2], а також метод Войта–Янга–Буша [3], який забезпечує зменшення впливу ЦВЗ у разі його вбудовування на якість зображення, однак сумарна похибка відхилення координат точок відносно оригіналу в деяких випадках є досить суттєвою.

В роботі [4] запропоновано метод, який забезпечує зменшення сумарної похибки відхилення координат точок від оригіналу. Однак в деяких випадках максимальне відхилення точок досягає великих значень, яке може призвести до помітних спотворень окремих точок [5].

В зв'язку з цим певний інтерес викликає метод, наведений в роботі [6], в якому для забезпеченням зменшення впливу його вбудовування на відхилення точок зображення вбудовування бітів ЦВЗ здійснюється лише у ті матриці коефіцієнтів ДКП, зміна яких не приводить до таких відхилень. Для визначення придатних для вбудовування матриць запропоновано умови відбору з використанням граничного значення величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ. Однак актуальним залишається питання аналізу запропонованого методу щодо забезпечення стійкості до зловмисних атак.

## Метод вбудовування цифрових водяних знаків у векторні зображення

Проведемо дослідження стійкості до атак методу, який розглянуто у роботі [6].

Згідно з методом [6] зображення подається у вигляді одновимірного масиву $V$, в якому елементами є точки векторного зображення $V_l$, де $l = 1 \ldots N$, $N$ — кількість точок в масиві; $V_l = (X_l, Y_l)$, де $X_l$, $Y_l$ — значення координати точки $V_l$ векторного зображення.

Далі формуються матриці розміром $8 \times 8$ (тобто розмірність матриці $n = 8$) з кожних 64 координат точок масиву $V$, які позначено, як $C_i(x, y)$, де $i = 1 \ldots t$, $t$ — кількість сформованих матриць, $x$, $y$ — позиції координат в цій матриці.

Для кожної матриці $C_i(x, y)$ проводиться пряме двовимірне ДКП, в результаті чого отримуються матриці коефіцієнтів $F(u, v)$, де $u$, $v$ — позиції цих коефіцієнтів в матриці.

Для вбудовування одного біта ЦВЗ змінюється значення одного високочастотного (ВЧ) коефіцієнта

$F_i(u_1, v_1)$ матриці ДКП залежно від значень двох ВЧ-коефіцієнтів $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$.

Після вибору позицій трьох коефіцієнтів $F_i(u_1, v_1)$, $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$ проводиться перевірка придатності відповідної їм $i$-ї матриці $F_i(u, v)$ для вбудовування біта ЦВЗ:

$$\left|F_i(u_1, v_1) - F_i(u_2, v_2)\right| \le P_h; \tag{1}$$

$$\left|F_i(u_1, v_1) - F_i(u_3, v_3)\right| \le P_h. \tag{2}$$

Якщо матриця не відповідає умовам (1) та/або (2), вона пропускається і аналізується наступна. Якщо ж матриця відповідає цим умовам, проводиться вбудовування біта ЦВЗ.

Вбудовування бітів ЦВЗ $m_j$ в придатні матриці здійснюється таким чином. Якщо біт $m_j = 0$, то перевіряється умова

$$F_i(u_1, v_1) < \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2}. \tag{3}$$

Якщо умова (3) виконується, значення коефіцієнта $F_i(u_1, v_1)$ залишається без змін, інакше значення коефіцієнта $F_i'(u_1, v_1)$ у матриці $F_i'(u, v)$ з вбудованим бітом ЦВЗ отримується таким чином:

$$F_i'(u_1, v_1) = \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2} - P. \tag{4}$$

Величина $P$ використовується для забезпечення чіткої ідентифікації бітів ЦВЗ у разі витягування.

Якщо при вбудовуванні біт ЦВЗ $m_j = 1$, то перевіряється виконання такої умови:

$$F_i(u_1, v_1) > \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2}. \tag{5}$$

Якщо умова (5) виконується, то коефіцієнт $F_i'(u_1, v_1)$ буде дорівнювати значенню коефіцієнта $F_i(u_1, v_1)$, інакше

$$F_i'(u_1, v_1) = \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2} + P. \tag{6}$$

Після зміни коефіцієнтів проводиться обернене дискретне косинус-перетворення над матрицями змінених коефіцієнтів $F'(u, v)$.

Далі з отриманих матриць змінених координат точок $S(x, y)$ формується одновимірний масив точок векторного зображення $V'$.

Витягування ЦВЗ з векторного зображення проводиться таким чином. Спочатку з масиву точок векторного зображення з вбудованим ЦВЗ $V'$ формуються матриці $C_{i'}'(x, y)$ розміром $8 \times 8$, де $i' = 1 \ldots t'$, $t'$ — кількість сформованих матриць. Далі над матрицями $C'(x, y)$ проводиться пряме двовимірне ДКП.

Після вибору позицій трьох ВЧ-коефіцієнтів $F_{i'}'(u_1', v_1')$, $F_{i'}'(u_2', v_2')$ та $F_{i'}'(u_3', v_3')$ перевіряється виконання умов та визначається відповідне значення біту ЦВЗ $m_{j'}'$:

$$\begin{cases} m_{j'}' = 0, \text{ якщо } F_{i'}'(u_1', v')_1 < \dfrac{F_{i'}'(u_2', v_2') + F_{i'}'(u_3', v_3')}{2}; \\ m_{j'}' = 1, \text{ якщо } F_{i'}'(u_1', v')_1 > \dfrac{F_{i'}'(u_2', v_2') + F_{i'}'(u_3', v_3')}{2}. \end{cases} \tag{7}$$

Далі витягнуті біти $m_{j'}'$, $j' = 1 \ldots q'$ перетворюються у формат подання ЦВЗ.

### Дослідження стеганографічної стійкості запропонованого методу

Аналіз стійкості запропонованого у роботі [6] методу проведемо з точки зору стійкості ЦВЗ до зловмисних атак.

Стеганографічні атаки поділяють на пасивні та активні [1]. Пасивні атаки спрямовані на виявлення факту присутності ЦВЗ у зображенні, зчитування даних ЦВЗ або визначення місця розташування ЦВЗ шляхом дослідження певних характеристик маркованого зображення. Такі атаки ніяк не впливають на зображення з ЦВЗ. Активні атаки проводяться з метою підміни або видалення ЦВЗ, а також зміни зображення для ускладнення витягування ЦВЗ. В результаті проведення таких атак зображення може бути зміненим.

Пасивні атаки на системи ЦВЗ, в основному, використовують статистичні методи стеганоаналізу зображень з ЦВЗ, які базуються на порушенні статистичних закономірностей оригінальних зображень. За такого підходу аналізуються статистичні характеристики зображення з ЦВЗ і визначається, чи схожі вони на характеристики зображень такого типу без ЦВЗ.

Такі методи стеганоаналізу використовують багато статистичних характеристик, серед яких найпоширенішими є оцінка ентропії та кореляції між елементами зображення. На основі цих оцінок можна приймати рішення про наявність чи відсутність ЦВЗ у зображенні, а також виявляти його місце розташування для витягування чи подальших атак. Тобто, якщо в блоці високорельованих точок зображення виявляється одна чи декілька точок з значними відхиленнями значень координат, можна припустити про присутність бітів ЦВЗ в цьому блоці зображення.

Стійкість запропонованого методу до таких атак забезпечується використанням ДКП, оскільки вбудовування бітів ЦВЗ проводиться зміною ВЧ-коефіцієнтів цього перетворення. У роботі [7] було проведено аналіз існуючих ортогональних перетворень з точки зору кореляційної теорії. Результати аналізу показали, що найоптимальніші результати для двовимірних матриць щодо кореляційних характеристик та показників ентропії забезпечує ДКП. Тобто, в результаті зміни одного коефіцієнта матриці $8 \times 8$ елементів будуть незначно змінені усі відповідні значення координат точок зображення. Це суттєво не вплине на якість зображення і забезпечить зниження ймовірності виявлення місця розташування ЦВЗ.

Окрім цього ДКП має швидкий алгоритм обчислення матриць коефіцієнтів, що в цілому забезпечує високу швидкодію методу.

Проаналізуємо тепер стійкість запропонованого методу до активних атак з боку зловмисника. У роботі [8] розглянуто можливі активні атаки на системи вбудовування ЦВЗ у векторні зображення. Серед яких атаки, спрямовані на підміну або видалення ЦВЗ, а також на зміну зображення для ускладнення витягування ЦВЗ додаванням додаткового шуму або видаленням/додаванням точок векторного зображення.

**Атаки, які проводяться з метою підміни ЦВЗ** частково можна віднести до вищерозглянутих пасивних атак, оскільки вони складаються з двох етапів, одним з яких є визначення місця розташування ЦВЗ для подальшої його підміни. Тобто для таких атак використовують методи пасивних атак.

Задачею атаки підміною ЦВЗ є те, щоб під час витягування правовласником ЦВЗ стегодетектор витягнув підмінений зловмисником ЦВЗ.

Згідно із запропонованим методом витягування ЦВЗ проводиться з використанням деяких параметрів, які є частиною секретного ключа. Наприклад, без знання правильного параметра $P_h$ зловмисник не зможе забезпечити витягування саме його ЦВЗ, оскільки воно визначає, в яких матрицях можуть знаходитись біти ЦВЗ.

**Атаки з видаленням ЦВЗ** є достатньо складними в реалізації, оскільки передбачають видалення ЦВЗ без спотворення зображення, а точніше із відновленням зображення до первинного вигляду. Для цього використовуються методи видалення шуму, перемодуляції, усереднення тощо.

Відповідно до запропонованого методу навіть знаючи усі дані для витягування ЦВЗ неможливо відновити зображення до первинного вигляду, оскільки для вбудовування бітів ЦВЗ можуть бути замінені значення ВЧ-коефіцієнтів на інші, без можливості відновлення. Також вбудовування ЦВЗ проводиться у певні блоки таким чином, щоб зміна їх в подальшому призвела до деградації зображення.

**Атака внесенням додатково шуму** зловмисником передбачає зміну усіх або деяких координат точок зображення, або ж зміну коефіцієнтів ДКП зображення для руйнування або знищення ЦВЗ. Оцінка стійкості методу до внесення шуму може визначатись як максимальний рівень зміни зна-

чень координат точок зображення чи коефіцієнтів ДКП, за якого забезпечується розпізнавання усіх бітів вбудованого ЦВЗ.

Оскільки векторні зображення характеризуються різними системами координат, а отже, і форматами зображення їх значень, рівень шуму будемо оцінювати на рівні коефіцієнтів ДКП.

Для того, щоб оцінити стійкість методу до внесення шуму, розглянемо детально те, що визначає допустимий рівень шуму в запропонованому методі.

Згідно з методом максимально можлива різниця між коефіцієнтом $F_i(u_1, v_1)$ та середнім арифметичним коефіцієнтів $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$ може сягати величини $P_h$. Тобто, якщо зміна зображення внаслідок внесення шуму призведе до того, що ця різниця стане більшою ніж $P_h$, біти ЦВЗ будуть неправильно розпізнані, оскільки відповідні матриці будуть вважатися непридатними згідно з умовами придатності для вбудовування.

Однак для визначення максимально можливого рівня шуму потрібно врахувати таке. Для вбудовування біта ЦВЗ коефіцієнт $F_i(u_1, v_1)$ може бути змінений на середнє арифметичне коефіцієнтів $F_i(u_2, v_2)$ та $F_i(u_3, v_3)$ змінене на величину $P$. Оскільки у разі витягування проводиться відносне порівняння значень цих коефіцієнтів, величина $P$ в такому випадку забезпечує розпізнавання біта ЦВЗ. Тому у випадку зміни коефіцієнтів для вбудовування бітів ЦВЗ максимально можливий рівень шуму буде визначатися значенням величини $P$. Тобто, зміна координат точок зображення чи відповідних їм коефіцієнтів ДКП повинна бути такою, щоб виконувалась умова

$$\left| F'_{i'}(u'_1, v'_1)_{\text{атак}} - \frac{F'_{i'}(u'_2, v'_2)_{\text{атак}} + F'_{i'}(u'_3, v'_3)_{\text{атак}}}{2} \right| < P. \qquad (8)$$

Оскільки згідно з методом величина $P$ повинна бути меншою за $P_h$, в загальному випадку максимально можливий рівень шуму зі забезпеченням правильного розпізнавання усіх бітів ЦВЗ повинен відповідати умові (8).

**Атака шляхом видалення/додавання точок** зображення призводить до зміни кількості точок зображення. Це в деяких випадках негативно впливає на стійкість запропонованого методу. Суть проблеми полягає у тому, що, якщо зловмисник видалить точку, яка брала участь у вбудовуванні ЦВЗ, або ж додасть нову, біля такої точки, деякі біти ЦВЗ будуть неправильно розпізнані.

Причиною є те, що у разі витягування ЦВЗ з певного діапазону точок зображення, де були проведені такі дії, будуть сформовані матриці з іншими координатами, тобто будуть зміщені відносно не атакованого зображення з ЦВЗ. Тоді, згідно з методом, будуть сформовані матриці коефіцієнтів ДКП, які також будуть відрізнятися від матриць зображення, яке не було зміненим.

Зауважимо, що така атака вплине на розпізнавання бітів ЦВЗ тільки для тих матриць ДКП, які були сформовані зі зміщених матриць.

Взагалі стійкість до атаки видаленням/додаванням точок зображення досить складно забезпечити, оскільки зловмисник може видаляти/додавати точки в будь-якому місці зображення.

Тому пропонується для вбудовування вибирати такі об'єкти зображення, для яких зміна кількості точок призведе до часткової або повної їх деградації. Такими об'єктами можуть бути низькодеталізовані полігони, що сформовані декількома точками.

В такому випадку видалення зловмисником однієї з точок може призвести до сильного спотворення об'єкта. Для прикладу створимо такий полігон та видалимо одну точку. Результат видалення однієї з точок такого об'єкта зображено на рис. 1.

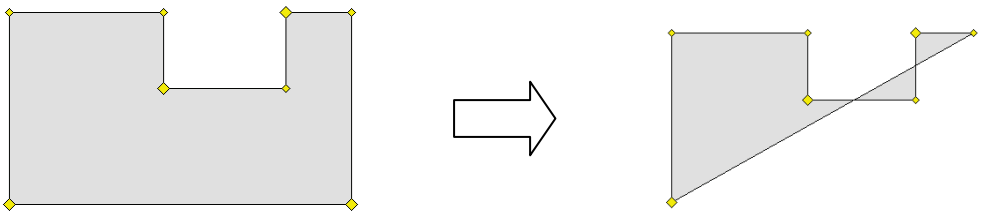
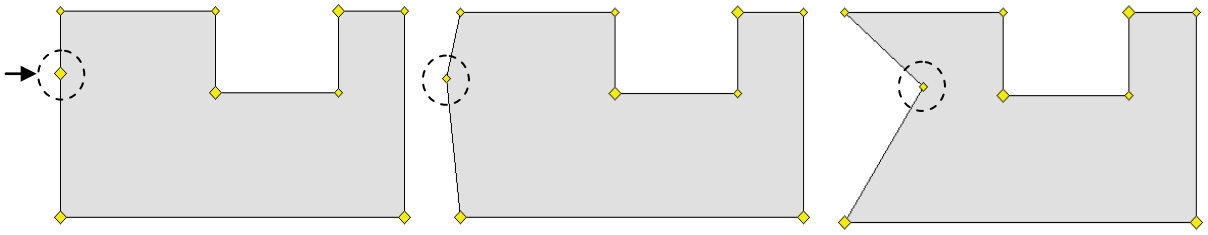


Рис. 1. Приклад об'єкта векторного зображення до та після видалення однієї точки зловмисником

Як видно з рис. 1, видалення лише однієї з точок полігону суттєво змінило його представлення, що можна вважати втратою цінності зображення. Тому правильне розпізнавання бітів ЦВЗ в такому випадку не є необхідним. Крім того, таке спотворення зображення може підтверджувати факт зловмисної атаки на зображення у вирішенні спорів.

Тепер проаналізуємо атаку шляхом додавання точок у зображення. Розглянемо декілька можливих випадків на прикладі нашого низькодеталізованого полігону. Вони будуть відрізнятись величиною відхилення внесеної точки відносно сусідніх, як показано на рис. 2.



а) б) в)

Рис. 2. Приклади додавання точок до полігону

На рис. 2а додаткова точка внесена на відрізок між двома точками полігону. В такому випадку ця точка зовсім не спотворює зображення, проте одна з її координат дорівнює значенню координат двох сусідніх точок. Таку точку можна легко визначити, порівнюючи між собою значення координат точок в межах одного об’єкта, і видалити перед проведенням процедури витягування ЦВЗ. Більше того, існуючі редактори векторних зображень і карт часто усувають таку надлишковість автоматично.

У другому випадку (рис. 2б) ситуація дещо складніша, оскільки координати точки відрізняються і при цьому зображення не сильно спотворене відносно оригіналу. Тому за таких змін деякі біти ЦВЗ можуть бути розпізнані неправильно.

Що стосується третього випадку (рис. 2в), то він схожий з видаленням точки, оскільки координати внесеної додаткової точки значно відрізняються від сусідніх і зображення значно спотворюється.

## Висновки

В роботі проведено аналіз запропонованого методу до найпоширеніших зловмисних атак, яких можуть зазнати векторні зображення з вбудованим ЦВЗ.

Результати аналізу показали, що завдяки використанню в методі двовимірного ДКП зберігається кореляція після вбудовування бітів ЦВЗ, що, в свою чергу, забезпечує стійкість до атак, які застосовують статистичні методи оцінювання і спрямовані на зчитування або визначення місця розташування ЦВЗ.

Використання в методі граничного значення відбору придатних для вбудовування матриць ДКП забезпечує додаткову стійкість методу до активних атак, спрямованих на видалення або підміну ЦВЗ.

Для забезпечення стійкості до атаки шляхом видалення/додавання точок запропоновано вбудовувати ЦВЗ у певні об’єкти, для яких зміна кількості точок призведе до їх деградації.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Основи комп’ютерної стеганографії : навч. посіб. / [В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук]. — Вінниця : ВДТУ. — 2003. — 143 с.

2. Zheng L. Research on Vector Map Digital Watermarking Technology / L. Zheng, Y. Jia, Q. Wang // First International Workshop on Education Technology and Computer Science — 2009. — P. 303—307.

3. Voigt M. Reversible watermarking of 2D vector data / M. Voigt, B. Yang and C. Busch // ACM Mutimedia and Security Workshop. — 2004. — P. 160—165.

4. Карпінець В. В. Вирішення проблеми погіршення якості векторних зображень при вбудовуванні цифрових водяних знаків / В. В. Карпінець, Ю. Є. Яремчук // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні — 2010. — № 1(20). — С. 72—82.

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

6. Карпінець В. В. Зменшення відхилень координат точок внаслідок вбудовування цифрових водяних знаків у векторні

зображення / В. В. Карпінець, Ю. Є. Яремчук // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні — 2010. — № 2(21). — С. 101—109.

7. Умняшкин С. В. Анализ эффективности использования дискретных ортогональных преобразований для цифрового кодирования коррелированных данных / С. В. Умняшкин, М. Е. Кочетков // Известия вузов. Электроника. — № 6. — 1998. — С. 79—84.

8. Zhou Y. Research of Robustness Evaluation Method for GIS Vector Data Digital Watermarking Algorithm / Y. Zhou, A. Li, G. Lv // Geoinformatics, 2010 18th International Conference on. — 2010. — P. 55—61.

Рекомендована кафедрою адміністративного та інформаційного менеджменту

Стаття надійшла до редакції 20.06.11
Рекомендована до друку 23.06.11

***Карпінець Василь Васильович*** — асистент, ***Яремчук Юрій Євгенович*** — доцент.
Кафедра адміністративного та інформаційного менеджменту, Вінницький національний технічний університет, Вінниця