УДК: 004.056.5

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

АНАЛІЗ СТІЙКОСТІ ДО ЗЛОВМИСНИХ АТАК МЕТОДУ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ

Проведено аналіз стійкості методу вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення до активних зловмисних атак, спрямованих на ускладнення витягнення ЦВЗ правовласником. Для цього були розглянуті поширені атаки на основі перетворень, таких як зміщення, поворот, масштабування та обсікання векторного зображення. Результати аналізу показали високий рівень стійкості методу до цих атак завдяки особливостям вбудовування ЦВЗ і використанню двовимірного дискретного косинусного перетворення.

Вступ

На сьогодні досить актуальною є задача захисту авторського права 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 [1].

Недоліком таких методів є спотворення зображення внаслідок вбудовування ЦВЗ. У роботі [2] запропоновано метод, який забезпечує збереження високого рівня якості зображення у разі вбудовування ЦВЗ [3].

Однак актуальним залишається питання аналізу запропонованого методу щодо забезпечення стійкості до зловмисних атак. У роботі [4] проведено дослідження стеганографічної стійкості методу до відомих активних і пасивних атак, спрямованих на зчитування, видалення або підміну ЦВЗ, а також на ускладнення витягування правовласником ЦВЗ шляхом додавання шуму або видалення/додавання точок векторного зображення. Проведений аналіз показав достатньо високий рівень стійкості запропонованого методу до таких атак.

Проте у роботі [4] було розглянуто стійкість цього методу не до всіх атак, що проводяться для ускладнення витягування правовласником ЦВЗ, зокрема, до перетворень векторних зображень.

Забезпечення стійкості стеганосистем ЦВЗ до таких атак є досить важливим, оскільки для проведення таких атак зловмисник не має необхідності виявляти місце розташування ЦВЗ, тому вони значно простіші в реалізації і є найпоширенішими [5].

Мета статті — провести аналіз стійкості запропонованого методу до цих атак для подальшого удосконалення методу.

Аналіз стійкості методу до атак на основі перетворень зображень

До найпоширеніших афінних перетворень зображення для проведення атак відносять зміщення, поворот, масштабування та обрізка векторного зображення.

Зміщення векторного зображення забезпечується зміною значень координат точок векторного зображення на однакову величину для осі абсцис та ординат таким чином:

$$\begin{cases} X' = X \pm dx; \\ Y' = Y \pm dy, \end{cases} \tag{1}$$

де X', Y' та X, Y — відповідно координати точок зміщеного та оригінального зображення, dx, dy — величини, на які змінюються координати X, Y, відповідно.

Кореляція між координатами точок повністю зберігається, тобто в цьому випадку зміна абсолютних значень координат точок не порушить кореляцію і між коефіцієнтами дискретного косинусного перетворення (ДКП).

Це пояснюється тим, що в результаті ДКП просторовий сигнал перетворюється в постійну складову (DC-коефіцієнт), що є середнім зваженим значення сигналу, і змінні компоненти (AC-коефіцієнти), які

представляють гармоніки сигналу. Тому в результаті зміщення значно може змінитися тільки DC-коефіцієнт, а значення AC-коефіцієнтів не зміняться. Оскільки суть методу полягає у вбудовуванні ЦВЗ шляхом відносної зміни частотних коефіцієнтів ДКП, можна припустити забезпечення достатньої стійкості запропонованого методу до такого типу атак.

Для аналізу стійкості запропонованого методу до атаки шляхом зміщення векторного зображення розглянемо приклад зміщення векторного зображення та його вплив на значення коефіцієнтів ДКП. Для аналізу створимо векторне зображення з 64 точок, яке показано на рис. 1.

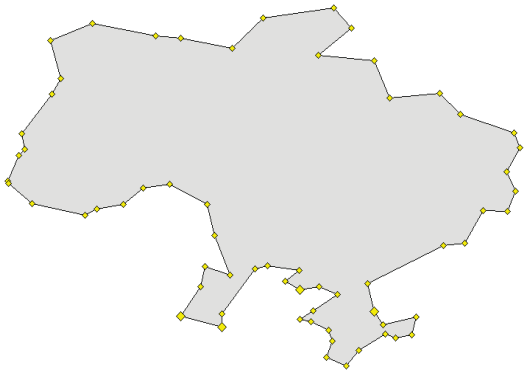

Рис. 1. Сформоване векторне зображення

Відповідно до методу з вузлових точок цього зображення сформуємо матрицю розміром 8×8 елементів і вбудуємо 1 біт ЦВЗ. Для проведення аналізу будемо розглядати тільки матрицю зі значеннями ординат точок зображення, яку показано на рис. 2.

$$\begin{pmatrix}
50.54704 & 50.54395 & 50.54667 & 50.54334 & 50.5455 & 50.54246 & 50.54455 & 50.54125 \\
50.54116 & 50.54183 & 50.5402 & 50.53792 & 50.53499 & 50.53382 & 50.53419 & 50.53296 \\
50.53226 & 50.53022 & 50.5302 & 50.52914 & 50.52693 & 50.52353 & 50.52062 & 50.51974 \\
50.51993 & 50.52346 & 50.5265 & 50.52022 & 50.52014 & 50.52702 & 50.52606 & 50.52488 \\
50.52501 & 50.525 & 50.52594 & 50.52638 & 50.52493 & 50.52169 & 50.52025 & 50.52047 \\
50.52072 & 50.5244 & 50.52616 & 50.5261 & 50.52354 & 50.52203 & 50.52057 & 50.52043 \\
50.52117 & 50.52347 & 50.52643 & 50.5284 & 50.52751 & 50.5274 & 50.5288 & 50.52965 \\
50.53087 & 50.53303 & 50.53482 & 50.53358 & 50.53394 & 50.53658 & 50.53963 & 50.54346
\end{pmatrix}$$

Рис. 2. Матриця координат точок зображення

Після проведення ДКП матриці координат точок отримаємо матрицю значень коефіцієнтів цього перетворення. Для подання результатів цього прикладу коефіцієнти ДКП розраховувались з точністю 5 десяткових знаків. У подальшому зі зміною коефіцієнтів розрахунки будуть проводитись з відповідною точністю.

Далі змістимо векторне зображення та оцінимо вплив на значення коефіцієнтів ДКП.

Задачею аналізу стійкості методу є оцінювання правильного розпізнавання бітів ЦВЗ після проведених атак на векторне зображення. Тому для об'єктивного оцінювання будемо проводити витягування біта ЦВЗ після кожної проведеної атаки.

Для цього спочатку вбудуємо у зображення один біт ЦВЗ «1», для чого оберемо три коефіцієнти з граничним значенням $P_h = 0,0005$. Приклад отриманої матриці ДКП з вибраними коефіцієнтами зображено на рис. 3.

$$\begin{pmatrix}
404.24063 & 0.00495 & -0.00266 & -0.00422 & -0.00224 & 0.00056 & 0.00108 & 0.00111 \\
0.02709 & 0.01457 & 0.00067 & 0.00378 & -0.00041 & 0.00109 & 0.00001 & 0.00195 \\
0.05058 & -0.00601 & 0.00326 & -0.00027 & 0.00160 & 0.00063 & -0.00108 & 0.00159 \\
0.00238 & 0.00196 & -0.00418 & 0.00027 & 0.00150 & 0.00054 & -0.00127 & 0.00110 \\
0.01401 & -0.00779 & 0.00348 & 0.00050 & -0.00193 & -0.00009 & 0.00146 & 0.00155 \\
-0.00707 & -0.00707 & -0.00076 & 0.00067 & -0.00220 & 0.00067 & 0.00126 & 0.00093 \\
-0.00073 & 0.00435 & -0.00150 & 0.00067 & 0.00133 & -0.00022 & 0.00029 & 0.00064 \\
-0.00143 & 0.00514 & -0.00267 & 0.00169 & 0.00506 & 0.00055 & -0.00097 & 0.00075
\end{pmatrix}$$

$F_i(u_2, v_2)$

$F_i(u_3, v_3)$

$F_i(u_1, v_1)$

Рис. 3. Вибір трьох коефіцієнтів ДКП для вбудовування біту ЦВЗ

Згідно з методом [2] значення обраних коефіцієнтів відповідають умовам для вбудовування бі-

та ЦВЗ «1», тому ніяких змін коефіцієнтів проводити не будемо.

Виконаємо зміщення векторного зображення, як показано на рис. 4.

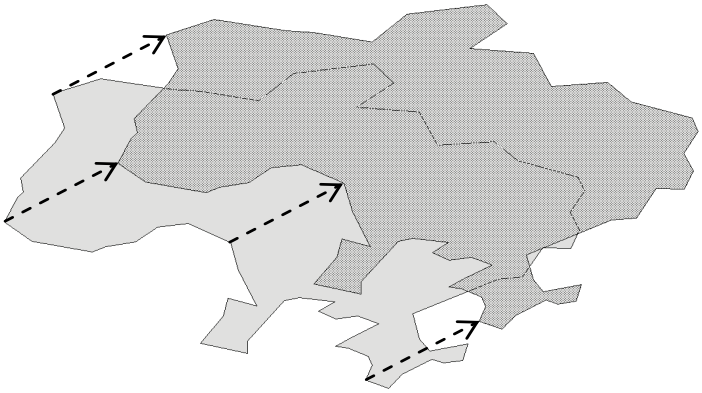

Рис. 4. Зміщення векторного зображення відносно оригіналу

Згідно з виразом (1) зміщеному зображенню відповідають координати, змінені на однакову величину.

Проведемо ДКП над матрицею координат точок зміщеного зображення для отримання матриці коефіцієнтів перетворення. Особливістю ДКП є те, що, якщо різниця між сусідніми значеннями координат точок не змінилася, відповідні АС-коефіцієнти також залишаться без змін. Зміниться тільки DC-коефіцієнт, який згідно з методом не приймає участі у вбудовуванні ЦВЗ, оскільки значення координат точок були змінені.

Оскільки обрані коефіцієнти для вбудовування біта ЦВЗ не змінилися взагалі, можливо чітко розпізнати вбудований біт ЦВЗ.

Такий результат показує, що запропонований метод завдяки особливостям ДКП є не чутливим до зловмисних атак шляхом зміщення зображення в координатній сітці.

Поворот зображення в просторі забезпечується завдяки перетворенню координат точок таким чином:

$$\begin{cases} X' = X\cos\alpha + Y\sin\alpha; \\ Y' = Y\cos\alpha - X\sin\alpha, \end{cases} \tag{2}$$

де α — кут повороту точок зображення.

Таку систему рівнянь також можна зобразити в матричному вигляді

$$[X', Y'] = [X, Y] \cdot \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}. \tag{3}$$

З виразу (3) видно, що для повороту зображення координати точок векторного зображення змінюються не на однакову величину одна відносно другої, як у випадку зі зміщенням, тому значення коефіцієнтів ДКП також будуть відрізнятися порівняно з коефіцієнтами оригінального зображення. Проте існує певна залежність між величинами зміни координат точок зображення, оскільки внаслідок повороту змінюються координати усіх точок.

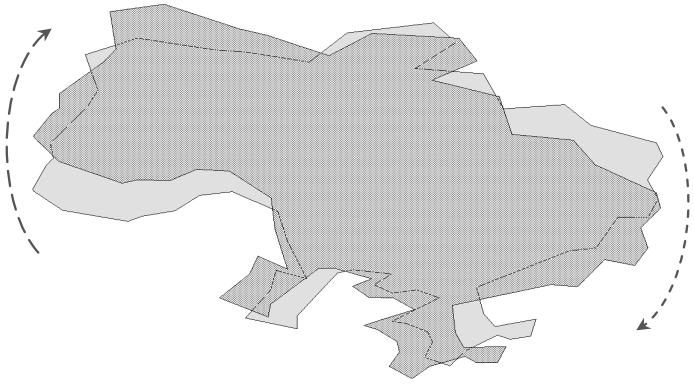

Рис. 5. Оригінальне та повернене зображення

Виконаємо поворот зображення на кут $\alpha = 10°$ відносно центра, як зображено на рис. 5.

На рис. 6 показано матрицю, елементами якої є різниці між координатами точок повернутого зображення та оригіналу.

Далі проведемо пряме ДКП і створимо матрицю отриманих коефіцієнтів, яку показано на рис. 7.

$$\begin{pmatrix} -0.00015 & -0.00009 & -0.00004 & 0.00002 & 0.00011 & 0.00014 & 0.0002 & 0.00024 \\ 0.0003 & 0.00038 & 0.00047 & 0.00053 & 0.00056 & 0.00053 & 0.00048 & 0.00049 \\ 0.00055 & 0.00052 & 0.00044 & 0.00039 & 0.00035 & 0.00039 & 0.00044 & 0.00041 \\ 0.00036 & 0.00032 & 0.00029 & 0.00032 & 0.00026 & 0.00023 & 0.00019 & 0.00008 \\ 0.00003 & -0.00003 & -0.00006 & -0.0001 & -0.0001 & -0.00007 & -0.00009 & -0.00013 \\ -0.00018 & -0.00016 & -0.00016 & -0.00017 & -0.00017 & -0.00017 & -0.00019 & -0.00023 \\ -0.00026 & -0.00024 & -0.00023 & -0.00023 & -0.00027 & -0.00035 & -0.00049 & -0.00058 \\ -0.00066 & -0.00072 & -0.00072 & -0.00063 & -0.00041 & -0.00035 & -0.0003 & -0.00023 \end{pmatrix}$$

Рис. 6. Матриця різниць координат поверненого та оригінального зображень

$$\begin{pmatrix} 404.23956 & 0.00579 & -0.00183 & -0.00496 & -0.00212 & 0.00058 & 0.00117 & 0.00104 \\ 0.00404 & 0.01525 & 0.00070 & 0.00463 & -0.00024 & 0.00096 & 0.00012 & 0.00200 \\ 0.05885 & -0.00031 & 0.00366 & -0.00010 & 0.00116 & 0.00128 & -0.00111 & 0.00132 \\ 0.00908 & 0.00165 & -0.00327 & 0.00071 & 0.00168 & 0.00059 & -0.00133 & 0.00105 \\ 0.02036 & -0.00460 & 0.00235 & -0.00011 & -0.00222 & -0.00011 & 0.00145 & 0.00143 \\ -0.00578 & -0.01005 & -0.00006 & 0.00064 & -0.00201 & 0.00038 & 0.00149 & 0.00114 \\ 0.00114 & 0.00653 & -0.00371 & 0.00066 & 0.00135 & -0.00020 & 0.00042 & 0.00052 \\ 0.00055 & 0.00386 & -0.00372 & 0.00160 & 0.00518 & 0.00056 & -0.00104 & 0.00073 \end{pmatrix}$$

Рис. 7. Матриця коефіцієнтів ДКП поверненого зображення

Як видно з рис. 7, внаслідок повороту зображення усі коефіцієнти ДКП змінили свої значення, але можна правильно розпізнати біт ЦВЗ, оскільки змінені значення вибраних трьох коефіцієнтів відповідають умовам розпізнавання біта «1» згідно з методом [2].

Таким чином, запропонований метод повороту зображення є достатньо стійким до зловмисної атаки.

Під час **масштабування** здійснюють збільшення або зменшення розмірів зображення згідно з перетвореннями

$$[X', Y'] = [X, Y] \cdot \begin{bmatrix} Kx & 0 \\ 0 & Ky \end{bmatrix}, \tag{4}$$

де Kx, Ky — масштабні коефіцієнти.

Якщо $Kx = Ky = K$, здійснюється перетворення подібності і зображення збільшується або зменшується в K разів. Відповідно, якщо обрати різні коефіцієнти Kx та Ky, то таке масштабування буде називатись розтягуванням або стисненням зображення по вертикалі чи горизонталі.

Виконаємо, для прикладу, масштабування обраного векторного зображення з коефіцієнтами $Kx = Ky = 1,3$, тобто в результаті воно збільшиться у 1,3 рази. Згідно з виразом (4) усі координати точок збільшаться у 1,3 рази, що, в свою чергу, приведе ще й і до відповідного зміщення усіх точок векторного зображення відносно оригіналу. Тому для того, щоб забезпечити зміну точок, необхідну тільки для масштабування зображення, виконаємо прив'язку зображення до певної точки. Масштабоване зображення показано на рис. 8.

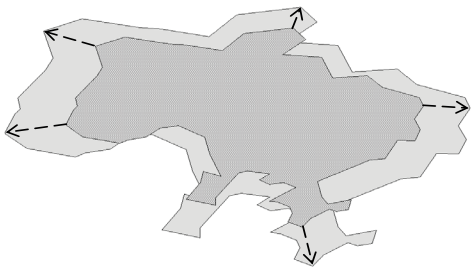

Рис. 8. Оригінальне та масштабоване у 1,3 рази зображення

Масштабованому зображенню буде відповідати матриця змінених координат точок. Матрицю різниць коор-

динат оригінального та масштабованого зображення показано на рис. 9.

$$\begin{pmatrix} -0.00819 & -0.00726 & -0.00808 & -0.00708 & -0.00773 & -0.00682 & -0.00744 & -0.00645 \\ -0.00643 & -0.00663 & -0.00614 & -0.00545 & -0.00457 & -0.00422 & -0.00434 & -0.00397 \\ -0.00376 & -0.00314 & -0.00314 & -0.00282 & -0.00216 & -0.00114 & -0.00026 & 0 \\ -0.00006 & -0.00112 & -0.00203 & -0.00014 & -0.00012 & -0.00218 & -0.0019 & -0.00154 \\ -0.00158 & -0.00158 & -0.00186 & -0.00199 & -0.00156 & -0.00058 & -0.00015 & -0.00022 \\ -0.00029 & -0.0014 & -0.00193 & -0.00191 & -0.00114 & -0.00069 & -0.00025 & -0.00021 \\ -0.00043 & -0.00112 & -0.00201 & -0.0026 & -0.00233 & -0.0023 & -0.00272 & -0.00297 \\ -0.00334 & -0.00399 & -0.00452 & -0.00415 & -0.00426 & -0.00505 & -0.00597 & -0.00712 \end{pmatrix}$$

Рис. 9. Матриця різниць координат масштабованого та оригінального зображень

Далі проведемо ДКП матриці координат точок масштабованого зображення. В результаті чого отримаємо матрицю коефіцієнтів, змінених відносно оригіналу. Матрицю отриманих коефіцієнтів ДКП показано на рис. 10.

Як видно з рис. 10, внаслідок масштабування зображення усі коефіцієнти ДКП змінили свої

$$\begin{pmatrix} 404.26544 & 0.00644 & -0.00346 & -0.00548 & -0.00291 & 0.00073 & 0.00141 & 0.00144 \\ 0.03521 & 0.01894 & 0.00087 & 0.00491 & -0.00054 & 0.00142 & 0.00002 & 0.00254 \\ 0.06576 & -0.00781 & 0.00423 & -0.00036 & 0.00208 & 0.00082 & -0.00141 & 0.00207 \\ 0.00310 & 0.00255 & -0.00543 & 0.00034 & 0.00195 & 0.00070 & -0.00166 & 0.00143 \\ 0.01821 & -0.01013 & 0.00452 & 0.00064 & -0.00251 & -0.00011 & 0.00189 & 0.00201 \\ -0.00919 & -0.00919 & -0.00098 & 0.00087 & -0.00286 & 0.00087 & 0.00164 & 0.00121 \\ -0.00095 & 0.00565 & -0.00195 & 0.00087 & 0.00173 & -0.00029 & 0.00038 & 0.00083 \\ -0.00186 & 0.00668 & -0.00347 & 0.00219 & 0.00657 & 0.00072 & -0.00127 & 0.00098 \end{pmatrix}$$

Рис. 10. Матриця коефіцієнтів ДКП повернутого зображення

значення. Що стосується вбудованого біта ЦВЗ, то можемо його правильно розпізнати, оскільки змінені значення вибраних трьох коефіцієнтів відповідають умові витягування біта «1».

Задача стійкості методу щодо атаки завдяки **відсіканню** векторного зображення пов'язана з тим, з яких боків і на скільки обрізується зображення, а також від того, яку частину зображення займає ЦВЗ і звідки починається вбудовування. Наприклад, якщо зловмисник відсіче зображення з усіх боків, а ЦВЗ було вбудовано, починаючи з перших координат точок, ЦВЗ буде неможливо витягти без оригіналу векторного зображення.

Ця задача може бути розв'язана шляхом вбудовування ЦВЗ лише у ті блоки зображення, видалення яких призведе до втрати цінності векторного зображення. Це можуть бути блоки, що розміщені ближче до центра. Проте в цьому випадку виникає задача знаходження першої точки блоку зображення, з якої починається відлік для вбудовування.

Для розв'язання цієї задачі, наприклад, для географічних векторних карт, пропонується робити прив'язку першої точки до так званих точок інтересу POI, які присутні в більшості векторних географічних карт. Точки POI можуть містити інформацію про назву населеного пункту, річки, вулиці, будівлі, парку тощо. Тому першою точкою для вбудовування можна обрати найближчу точку до POI. Така точка додатково може бути частиною секретного стеганоключа k, що взагалі підвищить стійкість запропонованого методу. Також слід зазначити, що можливість користувача створювати додаткові власні точки інтересу спрощує процедуру вибору та збереження такого ключа.

Висновки

У роботі проведено аналіз стійкості запропонованого методу вбудовування цифрових водяних знаків до активних зловмисних атак, спрямованих на ускладнення витягнення ЦВЗ правовласником. Для цього розглянуті поширені атаки на основі афінних перетворень, таких як зміщення, поворот, масштабування та обрізка векторного зображення.

Результати дослідження показали, що використання двовимірного ДКП дозволяє забезпечити

абсолютну стійкість методу до зміщення векторного зображення, а також достатньо високий рівень до повороту та масштабування зображення.

Достатній рівень стійкості запропонованого методу до відсікання зображення може забезпечуватись шляхом вбудовування бітів ЦВЗ у певні блоки зображення із використанням точок інтересу POI.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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.

2. 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.

3. 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 .

4. Карпінець В. В. Дослідження стеганографічної стійкості методу вбудовування цифрових водяних знаків у векторні зображення / В. В. Карпінець, Ю. Є. Яремчук // Вісник Вінницького політехнічного інституту. — 2011. — № 3. — С. 200—205.

5. 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