5. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова)/http://www.ssl.stu.neva.ru/psw/crypto/rostovtsev/ Erosh_Skuratov.pdf

Рецензент: Шелест М.Є
Надійшла 12.09.2011

УДК: 004.056.5

Карпінець В. В., Яремчук Ю. Є.

АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ 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 [1]. 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 при його вбудовуванні 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, представлений в роботі [6], в якому для забезпеченням зменшення впливу його вбудовування на відхилення точок зображення вбудовування бітів ЦВЗ здійснюється лише у ті матриці коефіцієнтів дискретного косинусного перетворення (ДКП), зміна яких не призводить до таких відхилень. Для визначення придатних для вбудовування матриць запропоновано умови відбору, з використанням граничного значення величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ. Це дало можливість зменшити рівень спотворення векторних зображень до 20 разів порівняно з відомим методом Войта-Янга-Буша. Однак, при цьому залишається питання як змінилася обчислювальна складність запропонованого методу.

Тому актуальним є аналіз обчислювальної складності запропонованого методу методу та порівняння з відомим методом.

Аналіз обчислювальної складності методу вбудовування ЦВЗ у векторні зображення на основі двовимірного ДКП

Проведемо дослідження обчислювальної складності запропонованого методу. Обчислювальна складність буде визначатися як O :

$$O = O_{вбуд.} + O_{вит.}, \quad (1)$$

де $O_{вбуд.}$ та $O_{вит.}$ – обчислювальна складність вбудовування та витягування ЦВЗ відповідно.

Обчислювальна складність алгоритму вбудовування ЦВЗ у зображення $O_{вбуд.}$ згідно методу буде визначатися як кількість арифметичних операцій, необхідних для вбудовування ЦВЗ. Для визначення обчислювальної складності алгоритму вбудовування ЦВЗ врахуємо основні кроки, з яких він складається, а саме: проведення прямого двовимірного ДКП, відбір придатних матриць, зміна коефіцієнтів ДКП та виконання оберненого ДКП.

Таким чином обчислювальна складність алгоритму вбудовування ЦВЗ буде дорівнювати:

$$O_{вбуд.} = (O_{ДКП\,8\times8} + O_{об.ДКП\,8\times8} + O_{Ph}) \cdot N_{матр.} + O_{вбуд.1біт} \cdot j, \quad (2)$$

де $O_{ДКП\,8\times8}$ та $O_{об.ДКП\,8\times8}$ – відповідно обчислювальна складність прямого та оберненого ДКП для однієї матриці, O_{Ph} – обчислювальна складність перевірки придатності однієї матриці ДКП, $N_{матр.}$ – кількість матриць розміром 8×8, $O_{вбуд.1біт}$ – обчислювальна складність вбудовування одного біту ЦВЗ і одну матрицю ДКП, j – кількість біт ЦВЗ.

Обчислювальна складність витягування ЦВЗ $O_{вит.}$ визначається як кількість арифметичних операцій, необхідних для виконання основних кроків алгоритму, серед яких виконання прямого ДКП, визначення придатних матриць для вбудовування та витягування бітів ЦВЗ. $O_{вит.}$ буде визначатися, як:

$$O_{вит.} = (O_{ДКП\,8\times8} + O_{Ph}) \cdot N_{матр.} + O_{вит.1біт} \cdot j \quad (3)$$

де $O_{вит.1біт}$ – обчислювальна складність витягування одного біту ЦВЗ з однієї матриці коефіцієнтів ДКП.

Оскільки кількість операцій напряму залежить від розміру ЦВЗ j та розміру векторного зображення, тобто кількості матриць $N_{матр.}$, обчислювальну складність будемо розраховувати для виконання вбудовування одногу біту ЦВЗ у одну матрицю ДКП, для чого знадобиться 64 координати точок векторного зображення. Тоді обчислювальна складність для вбудовування ти витягування буде мати вигляд:

$$O_{вбуд.1матр.} = O_{ДКП\,8\times8} + O_{Ph} + O_{вбуд.1біт} + O_{об.ДКП\,8\times8}, \quad (4)$$

$$O_{вит.1матр.} = O_{ДКП\,8\times8} + O_{Ph} + O_{вит.1біт}. \quad (5)$$

Визначимо обчислювальну складність процесів вбудовування та витягування ЦВЗ згідно з запропонованим методом, які використовують арифметичні операції додавання, віднімання, множення та ділення. При цьому при визначенні обчислювальної складності будемо враховувати будемо враховувати операції додавання та множення, а операції віднімання та ділення зводити до цих операцій, оскільки вони мають приблизно однакову обчислювальну складність, що і відповідні операції додавання та віднімання. Операції логічного порівняння, присвоєння, читання та запису даних в пам'ять будемо вважати нехтовно малими і не враховувати при визначення обчислювальної складності. Виходячи з цього будемо визначати обчислювальну складність вбудовування та витягування ЦВЗ для однієї матриці ДКП, як:

$$O = O_{мн.} + O_{дод.}, \quad (6)$$

де $O_{мн.}$ – кількість операцій множення, $O_{дод.}$ – кількість операцій додавання.

Згідно з запропонованим методом для кожних 64 координат точок векторного зображення, з яких попередньо сформовані матриці розміром 8×8, виконується ДКП. Обчислювальна складність двовимірного ДКП за цією формулою буде $O_{ДКП8\times8} = 57344_{мн.} + 8512_{дод.}$, що сумарно складає 65856 операцій множення та додавання.

Однак двовимірне ДКП можна проводити за допомогою одновимірного, яке проводиться спочатку для рядків матриці, а потім для стовпців, що значно пришвидшує виконання ДКП. Тому для швидкого перетворення зображення в частотне представлення рекомендується використовувати швидке дискретне косинус-перетворення, яке виконується за допомогою множення матриць:

$$F_i = DCT \cdot C \cdot DCT^T, \tag{7}$$

$$DCT = \begin{cases} \frac{1}{\sqrt{n}}, при\ \ u = 0, 0 \le v \le n-1; \\ \sqrt{\frac{2}{n}} \cdot \cos\left[\frac{\pi \cdot u \cdot (2v+1)}{2n}\right], при\ 1 \le u \le n-1,\ 0 \le v \le n-1, \end{cases} \tag{8}$$

де F – матриця коефіцієнтів ДКП; DCT – трансформаційна матриця ДКП розмірністю $n \times n$, елементи якої визначаються за формулою (8); C_i – матриця координат точок зображення розмірністю $n \times n$, де $i = 1..t$, t – кількість сформованих матриць; DCT^T – транспонована матриця DCT.

При цьому слід використовувати тимчасовий масив для зберігання результату множення $TMP = DCT \cdot C_i$. Для отримання результату ДКП потрібно помножити матрицю TMP на DCT^T.

Таким чином, обчислювальна складність виконання швидкого ДКП складає $O_{ДКП8\times8'} = 1024_{мн.} + 896_{дод.}$.

Порівнюючи ці результати з обчислювальною складністю ДКП у роботі [6] видно, що обчислювальна складність швидкого ДКП приблизно у 32 рази менша. Тому для розрахунків обчислювальної складності алгоритмів вбудовування та витягання ЦВЗ будемо використовувати обчислювальну складність швидкого ДКП $O_{ДКП8\times8'}$.

Згідно алгоритму вбудовування ЦВЗ після проведення двовимірного ДКП виконується визначення придатності матриць для вбудовування ЦВЗ. При цьому перевіряється виконання двох умов з P_h [6], що визначають придатність матриці ДКП для вбудовування біту ЦВЗ. Для цього потрібно виконати 2 операції множення та дві операції додавання. Таким чином $O_{Ph} = 2_{мн.} + 2_{дод.}$.

Наступним кроком алгоритму вбудовування ЦВЗ після перевірки матриці на придатність є вбудовування біту ЦВЗ, шляхом перевірки умов для вбудовування ЦВЗ залежно від біту ЦВЗ та можливої зміни значень коефіцієнтів, кожна з яких потребує виконання однієї операції множення та двох додавань, тобто $O_{вбуд.1бит} = 1_{мн.} + 2_{дод.}$

Далі за алгоритмом виконується обернене ДКП, яке також має швидку формулу обчислень шляхом множення матриць і вимагає таку ж кількість арифметичних операцій, як і пряме двовимірне ДКП, тобто $O_{об.ДКП8\times8'} = 1024_{мн.} + 896_{дод.}$.

Таким чином, обчислювальна складність методу вбудовування ЦВЗ для вбудовування одного біту ЦВЗ у матрицю із 64 координат точок зображення складає $O_{вбуд.1матр.} = 2051_{мн.} + 1796_{дод.}$.

Як видно з результатів оцінювання, при вбудовуванні одного біту ЦВЗ у матрицю коефіцієнтів ДКП розміром 8×8, 99,7% усіх арифметичних операцій складають пряме та

обернене ДКП, а обчислювальна складність самого алгоритму вбудовування бітів ЦВЗ шляхом зміни коефіцієнтів є відносно незначною з точки зору обчислювальної складності.

Обчислювальну складність алгоритму витягування ЦВЗ також проведемо для однієї матриці 64 координат точок зображення з одним вбудованим бітом ЦВЗ.

Як і у випадку з вбудовуванням, на першому етапі потрібно провести пряме двовимірне ДКП, яке вимагає $O_{ДКП8\times8'} = 1024_{мн.} + 896_{дод.}$. Далі проводиться перевірка умов для визначення придатності матриці для вбудовування ЦВЗ, аналогічно процесу вбудовування, тобто $O_{Ph} = 2_{мн.} + 2_{дод.}$.

Після перевірки придатності матриці для вбудовування ЦВЗ виконується витягування біту ЦВЗ [6]. Для цього потрібно перевірити одну умову, для виконання якої потрібно виконати одну операцію множення та додавання, тобто $O_{вит.1біт} = 1_{мн.} + 1_{дод.}$.

Таким чином обчислювальна складність алгоритму витягування одного біту ЦВЗ з однієї матриці 64 координат точок зображення буде дорівнювати: $O_{вит.1матр.} = 1027_{мн.} + 899_{дод.}$.

Як і у випадку вбудовування, при витягуванні теж основну частину арифметичних операцій складає виконання двовимірного ДКП.

Загальна кількість операцій для вбудовування ЦВЗ у 2 рази більша ніж для витягування ЦВЗ, що пояснюється тим, що при вбудовуванні ДКП виконується два рази, а при витягуванні лише один.

Порівняємо обчислювальну складність запропонованого методу з відомим методом Войта-Янга-Буша [3], що базується на одновимірному ДКП. Для цього проведемо оцінювання обчислювальної складності методу Войта-Янга-Буша. Оцінювати будемо також з розрахунку вбудовування та витягування одного біту ЦВЗ. Згідно з методом Войта-Янга-Буша, один біт ЦВЗ вбудовується в одновимірний масив з 8 координат точок векторного зображення. Обчислювальну складність для вбудовування та витягування одного біту ЦВЗ можна обчислити за такими виразами:

$$O_{вбуд.1мас.Войт} = O_{ДКП8} + O_{вбуд.1біт} + O_{об.ДКП8}, \quad (9)$$

$$O_{вит.1мас.Войт} = O_{ДКП8} + O_{вит.1біт}. \quad (10)$$

де $O_{ДКП8}$ та $O_{об.ДКП8}$ - пряме та обернене одновимірне ДКП для масиву з 8 точок зображення.

На першому етапі проводиться одновимірне ДКП, яке потребує виконання 472 операцій множення та 64 операцій додавання, тобто $O_{ДКП8} = 472_{мн.} + 64_{дод.}$.

Після проведення ДКП виконується процедура пошуку максимального коефіцієнта серед 6 коефіцієнтів масиву. Після чого залежно від біту ЦВЗ останній коефіцієнт може бути збільшений на значення максимального коефіцієнта, тобто виконується одна операція додавання $O_{вбуд.1біт.Войт} = 1_{дод.}$.

Після вбудовуванні бітів ЦВЗ проводиться обернене одновимірне ДКП, обчислювальна складність якого дорівнює прямому ДКП, тобто $O_{об.ДКП8} = 472_{мн.} + 64_{дод.}$.

Таким чином обчислювальна складність алгоритму вбудовування ЦВЗ згідно методу Войта-Янга-Буша становить $O_{вбуд.1мас.Войт} = 944_{мн.} + 129_{дод.}$ (оп.).

Обчислювальна складність алгоритму витягування ЦВЗ буде складатися з виконання прямого одновимірного ДКП $O_{ДКП8} = 472_{мн.} + 64_{дод.}$ (оп.). Після чого проводиться порівняння останнього коефіцієнта з 6-ма іншими коефіцієнтами. В результаті перевірки приймається рішення про присутній біт ЦВЗ. В даному випадку потрібне виконання тільки 6 операцій логічного порівняння.

Отже обчислювальна складність алгоритму витягування ЦВЗ за методом Войта-Янга-Буша дорівнює $O_{вит.Умас.Войт} = 472_{мн.} + 64_{дод.}$, що у 2 рази менше ніж при вбудовуванні ЦВЗ, оскільки як і у випадку запропонованого методу більше 99% арифметичних операцій складає виконання ДКП.

Проведемо порівняння обчислювальної складності методу, запропонованого в роботі [6], та методу Войта-Янга-Буша. Хоча операції множення та додавання відрізняються по своїй складності виконання, з точки зору швидкості обчислень цих операцій сучасними процесорами можна вважати їх рівними, оскільки виконання кожної з них відбувається в межах одного такту.

Для можливості проведення порівняння обчислювальної складності запропонованого методу з методом Войта-Янга-Буша врахуємо те, що хоча операції множення і є більш складними ніж операції додавання з точки зору обчислювальної складності, але сучасні процесори виконують кожну з них в межах одного такту. Тому швидкість виконання операцій множення та додавання будемо вважати однаковою.

Враховуючи це, метод вбудовування ЦВЗ з відбором придатних для вбудовування матриць ДКП [6] має у 3,55 разів більшу обчислювальну складність процесу вбудовування ЦВЗ та у 3,14 разів алгоритму витягування ЦВЗ порівняно з методом Войта-Янга-Буша.

При цьому слід зазначити, що запропонованого метод дає суттєві переваги, оскільки в ньому використовується двовимірне ДКП і 1 біт ЦВЗ вбудовується у блок з 64 коефіцієнтів, а це забезпечує менший рівень спотворень та кращу стійкість то пасивних атак шляхом статистичного дослідження.

Також слід зазначити, що обчислювальну складність на рівні методу Войта-Янга-Буша можна забезпечити і згідно запропонованого методу, якщо в кожну матрицю розміром 8×8 вбудовувати не один біт, а більше. Наприклад, якщо вбудовувати в матрицю 8 біт, то обчислювальна складність алгоритму вбудовування ЦВЗ згідно запропонованого методу зменшиться приблизно у 7 разів, і буде дорівнювати 2041 оп. В такому випадку запропонованого метод буде мати обчислювальну складність меншу ніж метод Войта-Янга-Буша приблизно у 1,88 разів і при цьому буде забезпечувати менший рівень спотворення зображення за рахунок використання двовимірного ДКП.

Для кращого представлення на рисунку 1 показано графіки залежностей обчислювальної складності та сумарної похибки від кількості бітів ЦВЗ, вбудованих у 64 точки векторного зображення для обох методів.

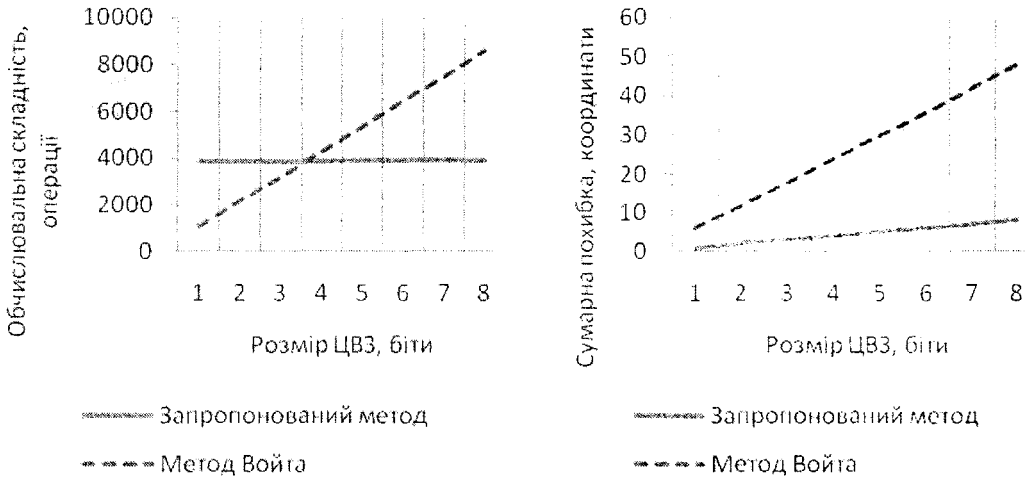

Рис. 1. Залежність обчислювальної складності та сумарної похибки від кількості бітів для запропонованого методу та методу Войта-Янга-Буша

З рисунку 1 видно, що для методу Войта-Янга-Буша спостерігається пропорційне збільшення обчислювальної складності та сумарної похибки відхилень координат точок зі збільшенням кількості бітів ЦВЗ. При цьому для запропонованого в роботі [6] методу, у випадку вбудовування більше ніж одного біту ЦВЗ у одну матрицю з 64 координат, обчислювальна складність збільшується незначно.

Це пояснюється тим, що незалежно від кількості бітів ЦВЗ ДКП, яке складає більше 90% обчислювальної складності алгоритму вбудовування ЦВЗ, виконується лише один раз. А згідно методу Войта-Янга-Буша для вбудовування кожного біту ЦВЗ потрібно виконувати одновимірне ДКП для масиву з 8 координат точок.

Сумарна похибка для запропонованого методу також збільшується зі збільшенням кількості біт ЦВЗ, однак навіть при вбудовування 8 бітів ЦВЗ рівень спотворення залишається нижчим.

Висновки

Проведений аналіз обчислювальної складності запропонованого методу вбудовування ЦВЗ показав, що вбудовування ЦВЗ потребує у 2 рази більше арифметичних операцій, ніж для витягування, що пояснюється необхідністю виконання за методом більше 90% операцій для проведення ДКП, яке при вбудовуванні виконується два рази, а при витягуванні ЦВЗ лише один. Також було проведено порівняння обчислювальної складності з відомим методом Войта-Янга-Буша, результати якого показали, що запропонований метод має у 3 рази більшу обчислювальну складність процесу вбудовування та витягування ЦВЗ. Однак запропонований метод дає суттєві переваги, оскільки в ньому використовується двовимірне ДКП і 1 біт ЦВЗ вбудовується у блок з 64 коефіцієнтів, а це забезпечує менший рівень спотворень та кращу стійкість то пасивних атак шляхом статистичного дослідження. Крім того, якщо згідно запропонованого методу в одну матрицю ДКП вбудовувати більшу кількість бітів ЦВЗ, то його обчислювальна складність буде незначно збільшуватись, в той час як складність методу Войта-Янга-Буша буде прямо пропорційно зростати кількості вбудовуваних ЦВЗ. Так, зокрема при вбудовуванні 8 бітів ЦВЗ запропонований метод при достатньому рівні стійкості буде забезпечувати майже у 2 рази меншу обчислювальну складність ніж метод Войта-Янга-Буша і при цьому буде мати менший рівень спотворення зображення внаслідок вбудовування ЦВЗ.

Список літератури

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.

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

4. Патент на корисну модель №62199, (51) МПК (2011) H03M 13/00. Спосіб захисту векторних зображень цифровими водяними знаками у вигляді електронного коду / В.В. Карпінець, Ю.Є. Яремчук. - № u2011 066640; заявл. 27.05.2011; опубл. 10.08.2011; Бюл. №15, 2011.

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

6. *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.

Рецензент: Скрипник Л.В.

Надійшла 12.09.2011