Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет

В. В. Карпінець, Ю. Є. Яремчук

МЕТОДИ ЗАХИСТУ ВЕКТОРНИХ ЗОБРАЖЕНЬ ЦИФРОВИМИ ВОДЯНИМИ ЗНАКАМИ

Монографія

Вінниця
ВНТУ
2013

УДК 681.3.067
ББК 32.973
К 26

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки, молоді та спорту України (протокол № 10 від 30.05.2012 р.)

Рецензенти:

В. О. Хорошко, доктор технічних наук, професор

О. Г. Корченко, доктор технічних наук, професор

Карпінець, В. В.

К 26 Методи захисту векторних зображень цифровими водяними знаками : монографія / В. В. Карпінець, Ю. Є. Яремчук. – Вінниця : ВНТУ, 2013. – 156 с.

ISBN 978-966-641-524-3

В монографії розглядаються питання зменшення рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків (ЦВЗ) при забезпеченні достатнього рівня стійкості до зловмисних атак та можливості витягування ЦВЗ без наявності оригіналу зображення. Запропоновано метод вбудовування ЦВЗ, який за рахунок використання двовимірного дискретного косинус-перетворення (ДКП) та особливих змін його високочастотних коефіцієнтів забезпечує зменшення рівня спотворення зображень при вбудовуванні ЦВЗ. Монографія розрахована на аспірантів та науковців, які займаються дослідженнями в галузі захисту інформації, а також на студентів ВНЗ.

УДК 681.3.067
ББК 32.973

ISBN 978-966-641-524-3

ЗМІСТ

ВСТУП

Завдяки розвитку комп'ютерних технологій сьогодні можна представляти багато різних видів інформації у цифровому вигляді. Одними з найпоширеніших таких видів є цифрові зображення. В зв'язку з цим все актуальнішою стає необхідність розв'язання задачі захисту авторських прав цифрових графічних зображень. Для цього використовуються стеганографічні методи вбудовування цифрових водяних знаків [1–5], що дають змогу маркувати об'єкти захисту для подальшого виявлення неправомірного використання зображення.

Залежно від задач, які має вирішувати стеганосистема, розрізняють такі типи ЦВЗ: тендітні, напівтендітні та стійкі (робастні) [2, 6–11]. Тендітні ЦВЗ використовуються для перевірки цілісності зображення, тому при найменшій зміні зображення їх вже неможливо виявити. Напівтендітні ЦВЗ витримують незначні модифікації зображення, проте нестійкі до зловмисних перетворень, тому їх використовують для виявлення атак на зображення. Стійкі ЦВЗ можуть протистояти більшості відомих атак на стеганографічну систему, тому саме їх використовують для захисту авторських прав на зображення.

Поширені на сьогодні стеганографічні методи [12–25] захисту растрових зображень для вбудовування стійких ЦВЗ в основному базуються на використанні статистичної та фізіологічної надлишковості інформації. При цьому вбудовування бітів ЦВЗ, в основному, відбувається зміною відтінків кольору точок.

У розвиток стеганографії значний внесок зробили вітчизняні вчені М. Є. Шелест, Г. Ф. Конахович, В. О. Хорошко, В. К. Задірака, Б. П. Русин, І. І. Маракова, А. А. Кобозєва, Н. В. Кошкіна, [1–11] та інші. Внесок зазначених вчених полягає у розробці та вдосконаленні стеганографічних методів приховування інформації у растрові графічні зображення.

Проте на сьогодні векторні зображення теж мають достатньо широке використання, зокрема, для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо.

Двовимірні векторні географічні карти у наш час дуже широко використовуються і мають важливе значення. Існує велика кількість ти-

пів карт з різним призначенням та точністю відображення, на створення яких витрачається багато часу та коштів. Використання векторних карт сьогодні дуже поширене – існує достатньо Інтернет-сервісів, які надають доступ до деталізованих карт усього світу, крім того, кожен може скористатися системою GPS-навігації за допомогою спеціального пристрою чи мобільного телефону, які також використовують карти у векторному форматі. В зв'язку з цим виникає проблема, пов'язана з можливістю нелегального копіювання та розповсюдження векторних зображень, які мають свого правовласника.

Оскільки у файлі векторних зображень зберігається інформація про координати точок та колір, з яких за допомогою формул формуються об'єкти, то вбудовувати цифровий водяний знак можна, наприклад, шляхом зміни координат точок. Вбудовування ЦВЗ за рахунок зміни кольору є неефективним, оскільки кількість кольорів об'єктів у векторному зображенні, в основному, є значно меншою, ніж кількість точок, з яких формуються відповідні об'єкти. [39, 40].

На сьогодні запропоновано низку методів [28–56], що дозволяють вбудовувати інформацію в зображення векторного формату. Як і для растрових зображень, методи вбудовування цифрових водяних знаків у векторні зображення можна розділити на декілька груп залежно від того, яким чином вбудовується інформація. За аналогією з методами растрових зображень, де існують «прямі» та «непрямі» методи [57], так само можна здійснити поділ і методів для векторних зображень. До першої групи можна віднести «прямі» методи, які вбудовують біти ЦВЗ шляхом зміни абсолютних значень координат точок згідно з певним алгоритмом [58, 63, 64]. До другої групи можна віднести методи вбудовування інформації в зображення шляхом представлення його у певній формі з використанням певного математичного перетворення [61].

Основною проблемою при вбудовуванні ЦВЗ є погіршення якості зображення [5, 17]. Якщо для растрових зображень це погіршення якості зображення внаслідок значної зміни відтінків пікселів, то для векторних зображень – це зміна контурів об'єктів, чи їх положення внаслідок зміни кількості та координат точок. Причому для векторних зображень, що відображають реальні об'єкти в масштабі (архітектурні споруди, механічні та електронні прилади, географічні карти тощо),

ця проблема є дуже актуальною, бо суттєва зміна координат точок може спотворити інформацію про існуючі об'єкти чи вплинути на їх створення.

Основною вимогою до стеганосистем, які вбудовують ЦВЗ у цифрові зображення, є забезпечення незмінності вбудованої інформації при спотворенні зображення-контейнера та мінімальний вплив методу вбудовування ЦВЗ на якість самого зображення [2, 14, 65]. Залежно від того, яка інформація потрібна системі для того, щоб виявити ЦВЗ – оригінал зображення, ЦВЗ, секретний ключ чи додаткова інформація, вони поділяються на чотири типи [1, 66, 67]: конфіденційні, напівконфіденційні, напіввідкриті та відкриті стеганосистеми. Стеганосистеми перших двох типів вимагають наявності оригіналу зображення чи ЦВЗ та знання секретного ключа. Напіввідкриті стеганосистеми виявляють ЦВЗ за допомогою секретного ключа, який залежить від оригіналу зображення. Відкриті стеганосистеми для своєї роботи, окрім секретного ключа, не вимагають ні знання оригінального зображення, ні вбудованого ЦВЗ. Незважаючи на те, що на сьогодні широкого застосування отримали стеганосистеми конфіденційного або напівконфіденційного типу, перспективними є дослідження та розробка відкритих систем цифрових водяних знаків, для яких, при витягуванні ЦВЗ, не потрібно мати оригінал зображення та ЦВЗ [68, 69].

Для відкритих стеганосистем, на відміну від конфіденційних чи напівконфіденційних, існує проблема необхідності більшої зміни зображення при вбудовуванні ЦВЗ для забезпечення можливості розпізнавання бітів ЦВЗ без оригіналу зображення, а тільки на основі самого зміненого зображення та стегоключа [70].

До стеганографічних методів, що є основою для відкритих стеганосистем та базуються на певних перетвореннях векторних зображень, відносять відомі методи Базіна-Барса-Маделана, Хе-Жу-Ванга, Солачідіса-Ніколаїдіса-Пітаса, Войта-Янга-Буша [54–58]. Проте загальною проблемою цих методів є помітне погіршення якості векторного зображення внаслідок вбудовування ЦВЗ. Тому актуальними є дослідження, спрямовані на розробку методів для відкритих стеганосистем, в яких вирішувалася б указана проблема.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ВЕКТОРНИХ ЗОБРАЖЕНЬ ЦИФРОВИМИ ВОДЯНИМИ ЗНАКАМИ

1.1 Загальні положення та вимоги до стеганосистем ЦВЗ

Завдяки розвитку комп'ютерних технологій сьогодні можна представляти багато різних видів інформації у цифровому вигляді. Одними з найпоширеніших таких видів є цифрові зображення. В зв'язку з цим все актуальнішою стає необхідність розв'язання задачі захисту авторських прав цифрових графічних зображень. Для цього використовуються стеганографічні методи вбудовування цифрових водяних знаків [1, 4], що дають змогу маркувати об'єкти захисту для подальшого виявлення неправомірного використання зображення.

Предметом вивчення цифрових водяних знаків є можливості маркування мультимедійної інформації з метою її ідентифікації, автентифікації, а також моніторингу її поширення і копіювання [2].

У системах з цифровими водяними знаками застосовуються методи, за допомогою яких одні дані приховуються в інших. ЦВЗ містять спеціальну інформацію (про час і місце його створення, про авторські права та ін.) і можуть бути розпізнані лише спеціальними засобами.

Основною вимогою [3] до систем цифрових водяних знаків є стійкість цифрової мітки до різноманітних трансформацій файла-носія (зміни формату, ущільнення, аналогового перетворення, цифрових обробок) та до спроб її видалення третіми особами. Іноді не менш важливою вимогою є невидимість ЦВЗ. Цифрові водяні знаки можуть бути настільки стійкими, що зберігаються після кількаразових перетворень форматів зображень і можуть бути виявлені навіть після сканування типографського офсетного відбитка.

Як правило, усі системи цифрових водяних знаків мають два типових блоки (рис. 1.1) [1]: схему внесення водяного знака і схему пошуку/витягання водяного знака.

Вхідною інформацією для схеми внесення водяного знака є цифровий об'єкт I, водяний знак W і стегоключ K (необов'язковий параметр). Водяний знак W може мати будь-який вигляд: число, текст, зображення та ін. Практично в усіх системах ЦВЗ передбачена наявність

одного або навіть декількох стегоключів, які необхідні для захисту водяних знаків від несанкціонованих змін. Виходом системи є цифровий об'єкт з вбудованим водяним знаком.

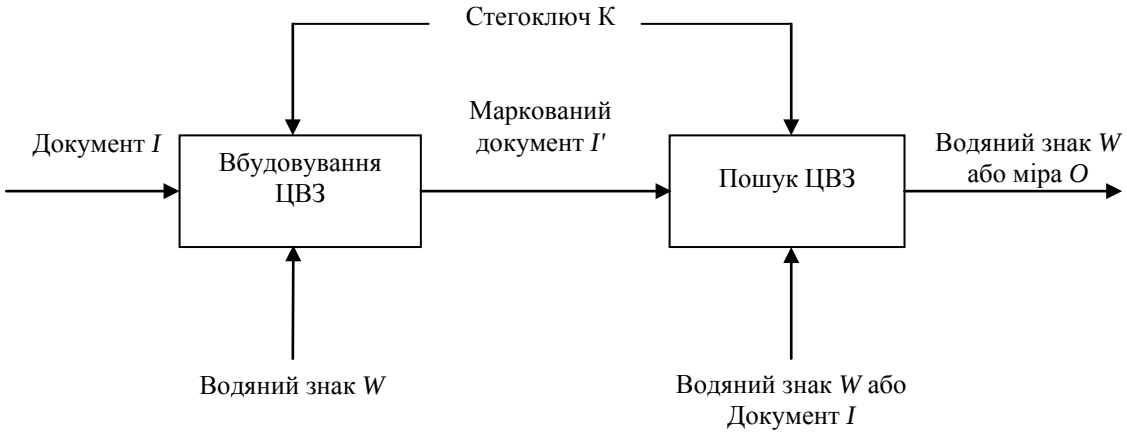


Рисунок 1.1 – Узагальнена схема системи ЦВЗ

Вихідними даними для процесу пошуку і/або видалення водяного знака є: цифровий об'єкт $\bar{I}'$ з водяним знаком (можливо, випадково або навмисно спотворений), стегоключ K і, в залежності від реалізованого методу, оригінальні копії даних I та/або водяного знака W. Результатом роботи схеми є витягнений водяний знак W або деяка оцінка O, за якою можна судити про ймовірне існування знака W в об'єкті $\bar{I}'$.

Подібна структура систем водяних знаків характерна для усіх видів цифрових даних: аудіо, зображень, відео, форматованих текстів, тривимірних моделей, параметрів мультиплікаційних моделей та ін.

Непомітність водяних знаків є загальною вимогою для всіх систем ЦВЗ [5]. Це означає, що перекручування, які вносяться водяними знаками, повинні залишатися нижче певного порога «видимості». Водяні знаки повинні бути невидимими не тільки для простого користувача, але й для експертів, озброєних досконалими методами статистичного аналізу.

З точки зору задач, які повинна вирішувати стеганосистема, існують такі основні вимоги до стеганосистем та варіанти їх забезпечення [5]:

1. Забезпечення безпеки систем ЦВЗ за допомогою стегоключів. У системах водяних знаків виділяють два рівні безпеки. Вищий рівень безпеки не дозволяє несанкціонованому користувачеві знайти і виділити водяні знаки. Другий рівень дозволяє будь-якому користувачеві

тільки виявляти факт присутності водяного знака, але інші дії з водяним знаком без знання ключа неможливі. Стегоключі відіграють важливу роль у захисті систем ЦВЗ від різного виду атак. Вимоги до системи керування ключами сильно залежать від застосувань, однак ключовий простір повинен бути достатньо великим для тотального перебору.

2. Можливість вирішення суперечок про право власності. У системі ЦВЗ повинні бути передбачені механізми визначення пріоритету проставлених водяних знаків у тому випадку, якщо в цифровому об'єкті їх знаходиться декілька і від різних джерел. Це, наприклад, може бути досягнуто введенням конструктивних обмежень на водяні знаки (наприклад, умови незворотності ЦВЗ) або додаткових функціональних можливостей (наявності тимчасових міток).

3. Доступність вихідних даних. Під час пошуку та витягання водяних знаків, копії оригіналу об'єкта та/або водяного знака можуть бути або доступними, або недоступними. Якщо вони доступні, то зазвичай реалізується система, яка під час витягання водяного знака використовує оригінал цифрових даних *I*. Такі системи мають велику завадостійкість не тільки до шумоподібних перекручувань, але і до геометричних. Однак у деяких застосуваннях (наприклад, під час моніторингу інформації) доступ до вихідної копії неможливий, а в інших (відео з водяними знаками) це практично неможливо через великий обсяг оброблюваних даних. Якщо в ранніх системах ЦВЗ для витягання водяних знаків зазвичай була потрібна вихідна копія контейнера, то в наш час спостерігається чітка тенденція розробки методів, у яких вона не потрібна.

4. Спосіб витягання і верифікації водяних знаків. Є два підходи до процесу внесення і відновлення ЦВЗ. Під час першого підходу водяний знак, що вноситься, вибирається з деякого допустимого набору, а під час його витягання перевіряється належність відновленого знака до цього набору. Під час другого – водяний знак вноситься шляхом модуляції деякої випадкової послідовності символів, а під час витягання вбудовані символи відновлюються шляхом демодуляції.

5. Завадостійкість водяних знаків до можливих випадкових перекручувань і/або навмисних модифікацій. Під час проектування систем часто керуються таким принципом: будь-яка успішно проведена атака на цифровий об'єкт із водяними знаками повинна знецінити комер-

ційне значення захищуваних даних. Дотепер ще не розроблено «ідеального» методу, який би забезпечив абсолютну захищеність водяних знаків. Тому практичні системи повинні прагнути до досягнення компромісу між такими суперечливими вимогами, як завадостійкість, невидимість та об'єм інформації у водяному знаку.

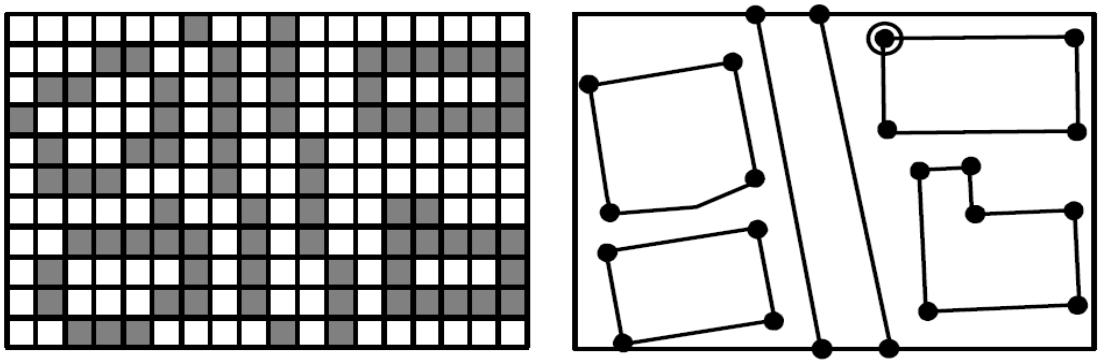
Якщо розглядати комерційні застосування стеганографії, то одним з найбільш перспективних напрямків її розвитку бачиться саме розвиток і застосування невидимих цифрових водяних знаків для захисту авторських прав на цифрові вироби. Поміщені у файл цифрові водяні знаки можуть бути розпізнані спеціальними програмами, які витягнуть з файла багато корисної інформації: коли створений файл, хто має авторські права, як вступити в контакт з автором.

Загальний процес маркування цифрового об'єкта водяними знаками може бути визначений як відображення такого вигляду [6]: $I \times K \times W \to \overline{I'}$, де I – вихідний цифровий об'єкт; W – водяний знак, K – стегоключ; $\bar{I}'$ – маркований цифровий об'єкт. Результатом роботи схеми детектування ЦВЗ може бути або витягнений водяний знак W, або деяка оцінка O, яка вказує на ймовірність того, що об'єкт $\bar{I}'$ є маркованим.

Залежно від задач, які має вирішувати стеганосистема, розрізняють такі типи ЦВЗ: тендітні, напівтендітні та стійкі (робастні) [7]. Тендітні ЦВЗ використовуються для перевірки цілісності зображення, тому при найменшій зміні зображення їх вже неможливо виявити. Напівтендітні ЦВЗ витримують незначні модифікації зображення, проте нестійкі до зловмисних перетворень, тому їх використовують для виявлення атак на зображення. Стійкі ЦВЗ можуть протистояти більшості відомих атак на стеганографічну систему, тому саме їх використовують для захисту авторських прав на зображення.

Поширені на сьогодні стеганографічні методи захисту растрових зображень для вбудовування стійких ЦВЗ, в основному, базуються на використанні статистичної та фізіологічної надлишковості інформації. При цьому вбудовування бітів ЦВЗ, в основному, відбувається зміною відтінків кольору точок.

Проте на сьогодні векторні зображення (рис. 1.2) теж мають достатньо широке використання, зокрема, для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо.



Растрове Векторне

Рисунок 1.2 – Приклади растрового та векторного зображень

Двовимірні векторні географічні карти у наш час дуже широко використовуються і мають важливе значення. Існує велика кількість типів карт з різним призначенням та точністю відображення, на створення яких витрачається багато часу та коштів. Використання векторних карт сьогодні дуже поширене – існує достатньо Інтернет-сервісів, які надають доступ до деталізованих карт усього світу, крім того, кожен може скористатися системою GPS-навігації за допомогою спеціального пристрою чи мобільного телефону, які також використовують карти у векторному форматі. В зв’язку з цим виникає проблема, пов’язана з можливістю нелегального копіювання та розповсюдження векторних зображень, які мають свого правовласника.

Оскільки у файлі векторних зображень зберігається інформація про координати точок та колір, з яких за допомогою формул формуються об’єкти, то вбудовувати цифровий водяний знак можна, наприклад, шляхом зміни координат точок. Вбудовування ЦВЗ за рахунок зміни кольору є неефективним, оскільки кількість кольорів об’єктів у векторному зображенні, в основному, є значно меншою, ніж кількість точок, з яких формуються відповідні об’єкти.

На сьогодні запропоновано низку методів, що дозволяють вбудовувати інформацію в зображення векторного формату. Як і для растрових зображень, методи вбудовування цифрових водяних знаків у векторні зображення можна розділити на декілька груп залежно від того, яким чином вбудовується інформація. За аналогією з методами растрових зображень, де існують «прямі» та «непрямі» методи [2], так само можна здійснити поділ і методів для векторних зображень. До

першої групи можна віднести «прямі» методи, які вбудовують біти ЦВЗ шляхом зміни абсолютних значень координат точок згідно з певним алгоритмом в так званій просторовій області. До другої групи можна віднести методи вбудовування інформації в зображення шляхом представлення його у певній формі з використанням певного математичного перетворення.

Загальний підхід методів першої групи щодо вбудовування ЦВЗ у векторні зображення схожий з тим, що використовується для растрових зображень. Якщо для растрових методів – це пряма зміна значень кольорів зображень, то для векторних – незначна зміна координат точок, з яких складається зображення. Тому для векторних зображень можна використовувати алгоритми вбудовування інформації, що використовуються для растрових методів. Це ж стосується і підходів щодо покращення стійкості «прямих» методів, наприклад, за допомогою алгоритму псевдовипадкового інтервалу або псевдовипадкової перестановки. Слід зазначити, що особливістю векторних зображень є можливість змінювати не тільки значення точок, а й їх кількість, на основі чого можна розробляти нові алгоритми вбудовування інформації.

Проаналізуємо існуючі на сьогодні методи, що вбудовують ЦВЗ у просторову область.

У роботі [12] автори для запропонованого методу використовують оновлений та модифікований алгоритм квадрадерева. При використанні цього алгоритму векторне зображення розділяється на трикутну сітку, що базується на щільності вершин, ЦВЗ вбудовується шляхом модифікації координат вершин трикутних сіток. В той самий час порядок вбудовування ЦВЗ визначається поділом трикутних сіток на рівні. Для того, щоб витягнути ЦВЗ, необхідно розділити зображення з ЦВЗ таким самим чином і після цього порівняти координати вершин з даними ЦВЗ.

Також відомий метод [13], згідно з яким пропонується додавати точки зображення, змінювати довжину, напрям та атрибути ліній для вбудовування ЦВЗ. Вставка точок та зміна ліній є дуже простим методом, що не забезпечує стійкості методу, а метод зміни напрямку ліній та атрибутів не є підходящим для точних векторних даних.

Автори методу [14] взяли за основу метод, що використовує PN-послідовність (PN – псевдо-шум) в якості ЦВЗ і складається зі значень від'ємного та додатного максимальних відхилень (похибки) та

вбудовують його в координати 2-х вимірних векторних карт. Витягування ЦВЗ здійснюється за допомогою релевантності PN-послідовності та даних, що були вбудовані.

У роботі [15] автори пропонують метод, згідно з яким векторна карта ділиться на послідовність сіток висотою в 4/3 допустимого відхилення координат точок, після чого в кожній сітці рисуються дві лінії довжиною 1/3 допустимого відхилення і позначаються як лінія 0 і лінія 1. ЦВЗ вбудовується шляхом переміщення вершин в сітці до лінії 0 чи лінії 1. Якщо вершина в області 0 і нам необхідно вбудувати 1, ми переміщаємо вершину в область 1. Нова позиція є симетричною до оригінальної позиції відносно діагоналі.

Відомий метод [16], згідно з яким векторне зображення ділиться навпіл та проводиться адаптивне регулювання на стійкість ЦВЗ відповідно до щільності точок векторного зображення. Після цього, враховуючи дозволену максимально допустиму похибку відхилень координат точок векторного зображення, вбудовується ЦВЗ в векторне зображення шляхом зміни координат вершин. Для того, щоб витягнути дані ЦВЗ, необхідно перевірити карту з подвійним порогом.

У роботі [17] автори пропонують метод, згідно з яким векторне зображення розкладається відповідно до характеристик полігону. Після цього проводиться аналіз векторного полігону, обираються необхідні для вбудовування елементи зображення та проводиться вбудовування ЦВЗ у вершини полігонів. Для того, щоб витягнути ЦВЗ, необхідною є наявність оригінального зображення та самого ЦВЗ, після аналізу яких виконується витягування ЦВЗ з вершин полігонів.

Також відомий метод [18] перевірки цілісності векторної карти. Метод базується на зворотній технології вбудовування крихкого ЦВЗ та використовує ущільнення даних без втрат для досягнення зворотності. Оригінал векторного зображення використовується при витягуванні ЦВЗ для виявлення найменших змін векторного зображення. Основним недоліком цього методу є те, що додавання або видалення вершин полігонів чи поліліній знищує можливість виявлення модифікації векторного зображення.

У роботі [19] запропоновано метод, який комбінує метод найменш значущого біта (НЗБ), метод запису топології просторових даних ГІС, а також шифрування ЦВЗ. Цей метод реалізований для приховування

псевдовипадково розповсюдженого ЦВЗ в файлах певного формату, що використовуються програмним забезпеченням GISArc/Info.

Також відомий метод [20], автори якого пропонують двошаровий алгоритм вбудовування стійких ЦВЗ. Цей алгоритм розділяє векторну карту на два прошарки, в кожну з яких вбудовується ЦВЗ шляхом зміни точок векторного зображення, використовуючи при цьому різні алгоритми зміни. Для витягування ЦВЗ, необхідно не виходячи за межі допустимого рівня спотворень розрахувати позиції ЦВЗ в кожному прошарку, визначити точки, в яких вбудовано ЦВЗ та порахувати середнє значення координат.

Основними недоліками розглянутих методів є забезпечення недостатнього рівня стійкості до зловмисних атак на векторні зображення, особливо до пасивних, що дозволяють визначити місце розташування ЦВЗ для можливого його подальшого видалення. Це пов'язано з низьким рівнем кореляції між сусідніми точками, які були змінені внаслідок вбудовування ЦВЗ, що також спричиняє помітні спотворення векторного зображення.

Суть «непрямих» методів вбудовування ЦВЗ у використанні математичних перетворень для представлення зображень у такій формі, особливості якої дають додаткові можливості для вбудовування ЦВЗ. Для растрових зображень такі перетворення дозволяють представити зображення у вигляді значень частот певного кольору та дозволяють виділити в зображенні більш значущі елементи від незначущих, якими можна знехтувати без помітних людському оку візуальних змін. Така особливість дає можливість модифікувати такі значення перетворення, зміна яких суттєво не вплине на якість зображення та забезпечить достатню стійкість зображення до навмисних спотворень, наприклад, ущільнення згідно з алгоритмом JPEG.

На сьогодні запропоновано декілька «непрямих» методів вбудовування інформації у векторні зображення, які також використовують математичні перетворення. При цьому вбудовування ЦВЗ відбувається шляхом зміни не координат точок, а, наприклад, їхніх частотних характеристик. Наприклад, використання методу тріангуляції Делоне дозволяє перетворити векторне зображення, що є набором точок з певними координатами, у цілісне двовимірне зображення. Це зображення формується шляхом з'єднання всіх точок між собою згідно з методом та представляється у вигляді сітки, де лінії між точками не

перетинаються. Такий підхід використовується для подальшого застосування частотного перетворення. Після цього відбувається зміна значень використаного перетворення для вбудовування бітів цифрового водяного знаку.

Основною проблемою при вбудовуванні ЦВЗ є погіршення якості зображення. Якщо для растрових зображень це погіршення якості зображення внаслідок значної зміни відтінків пікселів, то для векторних зображень – це зміна контурів об'єктів, чи їх положення внаслідок зміни кількості та координат точок. Причому для векторних зображень, що відображають реальні об'єкти в масштабі (архітектурні споруди, механічні та електронні прилади, географічні карти тощо), ця проблема є дуже актуальною, бо суттєва зміна координат точок може спотворити інформацію про існуючі об'єкти чи вплинути на їх створення.

Залежно від того, яка інформація потрібна системі для того, щоб виявити ЦВЗ – оригінал зображення, ЦВЗ, секретний ключ чи додаткова інформація, вони поділяються на чотири типи [1, 5]: конфіденційні, напівконфіденційні, напіввідкриті та відкриті стеганосистеми. Конфіденційні системи ЦВЗ вимагають наявності вихідних даних *I*. Існують дві модифікації подібних систем. Перша з них використовує вихідне зображення як підказку для витягання водяного знака *W* у цифрових, можливо перекручених, даних $\overline{I'}$. Функціонування таких систем можна описати як $\overline{I'} \times I \times K \to W$. Вважається, що такі системи є найбільш завадостійкими до будь-яких атак, тому що вимагають наявності секретного стегоключа К і видають мінімум інформації.

Напівконфіденційні системи ЦВЗ не вимагають вихідної копії об'єкта для виявлення водяного знака *W*. Схему їхньої роботи можна представити як $\bar{I}' \times K \times W \to \{0,1\}$.

Напіввідкриті системи ЦВЗ використовують стегоключ (або іншу додаткову інформацію для виявлення водяного знака), який залежить від вихідної копії даних: $\bar{I}' \times K(I) \to W$.

Відкриті системи ЦВЗ для своєї роботи не вимагають знання а ні оригінальної копії даних *I*, а ні вбудованого водяного знака *W*. Такі системи витягають водяний знак з маркірованих даних: $\bar{I}' \times K \to W$.

Для відкритих стеганосистем, на відміну від конфіденційних чи напівконфіденційних існує проблема необхідності більшої зміни зображення при вбудовуванні ЦВЗ для забезпечення можливості розпі-

знавання бітів ЦВЗ без оригіналу зображення, а тільки на основі самого зміненого зображення та стегоключа.

Враховуючи те, що основною вимогою до стеганосистем, які вбудовують ЦВЗ у цифрові зображення, є забезпечення незмінності вбудованої інформації при спотворенні зображення-контейнера та мінімальний вплив методу вбудовування ЦВЗ на якість самого зображення, доцільним є дослідження відомих методів вбудовування ЦВЗ у векторні зображення щодо рівня спотворення зображень внаслідок вбудовування ЦВЗ з урахуванням типу стеганографічної системи.

Також важливим є врахування механізму вбудовування цифрових водяних знаків у зображення та типу стеганографічної системи, яку представляють методи з точки зору необхідної інформації при витягування ЦВЗ.

1.2 Аналіз методів захисту векторних зображень з точки зору рівня спотворення внаслідок вбудовування ЦВЗ

Оскільки у «прямих» методів вбудовування ЦВЗ у просторову область векторних зображень існують проблеми, пов’язані з недостатнім рівнем стійкості до зловмисних атак, більший інтерес викликають методи, що при вбудовуванні ЦВЗ використовують математичні перетворення для представлення зображення у певному вигляді і забезпечують вищий рівень стійкості.

Виходячи з поставлених завдань дослідження, важливим є аналіз цих методів з точки зору рівня спотворення зображень внаслідок вбудовування ЦВЗ, а також можливості витягування ЦВЗ без наявності оригіналу зображення чи самого ЦВЗ.

У роботі [21] запропоновано метод вбудовування ЦВЗ, що базується на дискретному перетворенні Фур’є (ДПФ). Суть методу полягає у зміні координат точок, з яких сформовані закриті полігони векторних карт. Цей метод використовує особливості перетворення Фур’є для геометричних перетворень. ЦВЗ вбудовується у послідовність коефіцієнтів ДПФ, що відповідають масивам вершин закритих полігонів. Витягування бітів ЦВЗ проводиться з використанням адаптованого методу виявлення лінійної кореляції. Для витягування необхідною є наявність оригіналу векторного зображення, що дещо ускладню процедуру підтвердження авторства.

На основі цього методу у роботі [22] запропоновано вдосконалений метод вбудовування ЦВЗ у векторні зображення, який не потребує для витягування ЦВЗ оригіналу зображення. Однак це досягається шляхом значної зміни коефіцієнтів ДПФ, що в деяких випадках суттєво впливає на якість векторного зображення внаслідок вбудовування ЦВЗ.

Також на основі методу [22] в роботі [23] запропоновано метод вбудовування ЦВЗ, в якому вдосконалено процедуру витягування ЦВЗ. Суть вдосконалення полягає у забезпеченні кращого рівня правильності розпізнавання бітів ЦВЗ. Для цього використовується надлишковість вбудованих даних, а також розроблено метод визначення наявності ЦВЗ у зображенні шляхом перевірки лише одного багатокутника. Недоліком цього методу є те, що для витягування ЦВЗ виникає необхідність наявності його оригіналу.

Автори роботи [24] пропонують метод, що також базується на ДПФ. Згідно з методом спершу виконується перетворення координат точок в ціле значення, а потім перетворення ДПФ для масивів з 8 точок. ЦВЗ вбудовується шляхом зміни високочастотних коефіцієнтів. В роботі також проведений детальний аналіз рівня спотворень векторних зображень внаслідок вбудовування ЦВЗ, а також можливого розміру ЦВЗ. Недоліком цього методу є невеликий розмір вбудованого ЦВЗ, а також необхідність наявності оригіналу зображення при витягуванні ЦВЗ.

У роботі [25] запропоновано метод, який є оптимізацією попереднього методу [24]. Згідно з методом також з’єднуються 8 сусідніх точок, однак над ними виконується ДКП. Коефіцієнти, отримані в результаті цього перетворення, діляться на два діапазони – R1 і R2. Для кожного коефіцієнта з діапазону R2, якщо він не більший за максимальний елемент з R1, відбувається подвоєння його значення. Якщо цей коефіцієнт більший, ніж максимальне значення в R1, до нього додається максимальне значення з R1. Таким чином, ЦВЗ вбудовується шляхом зміни коефіцієнта R2. Цей метод забезпечує витягування без наявності оригіналу ЦВЗ, однак внаслідок вбудовування ЦВЗ можливі значні спотворення векторного зображення.

Також запропоновано метод [26], що вбудовує ЦВЗ в діапазон коефіцієнтів ДПФ та використовує практичний алгоритм витягування ЦВЗ. Для витягування ЦВЗ використовується коефіцієнт кореляції ви-

тягнутого і оригінального ЦВЗ. Недоліком цього методу є необхідність наявності оригіналу самого ЦВЗ.

Метод, поданий в роботі [27], також вбудовує ЦВЗ у векторні зображення на основі частотного перетворення. Для цього методу використовується дискретне вейвлет-перетворення (ДВП) над множиною координат точок ліній і площин. Вбудовування ЦВЗ проводиться шляхом зміни низькочастотних коефіцієнтів, що отримані в результаті вейвлет-перетворення, після чого виконується зворотне ДВП для отримання векторного зображення з вбудованим ЦВЗ. Недоліком запропонованого методу є значний вплив зміни низькочастотних коефіцієнтів на значення координат точок, а також те, що при видаленні однієї з точок векторного зображення буде неможливо розпізнати ЦВЗ.

У роботі [28] запропоновано метод захисту авторського права векторних зображень за допомогою цифрових водяних знаків Обуші-Уеда-Ендоха. Суть методу полягає у вбудовуванні ЦВЗ у частотну область представлення векторного зображення.

Для цього векторне зображення представляється як масив точок, які з'єднуються між собою за допомогою тріангуляції Делоне. В результаті утворюється двовимірна поверхня з трикутників, вершинами яких є усі точки векторного зображення, приклад якої показано на рис. 1.3.

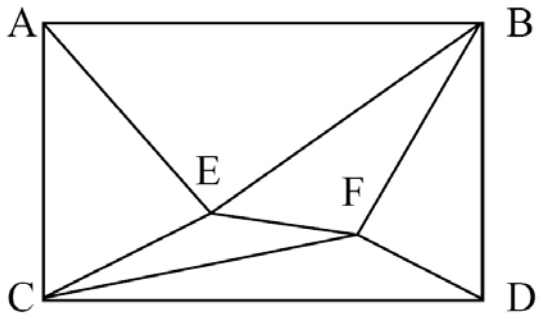


Рисунок 1.3 – Приклад частини сформованої поверхні після тріангуляції Делоне

Для представлення зображення у частотному вигляді проводиться послідовне перетворення частин утвореної поверхні за допомогою матриць Лапласа розміром n×n. Коефіцієнти отриманих матриць перетворення показують частоту появи певних значень довжин сторін трикутників. Приклад сформованої матриці показано на рис. 1.4.

$$
\begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array}
\begin{array}{c}
\begin{array}{cccccc} A & B & C & D & E & F \end{array} \\
\begin{bmatrix}
1 & -1/3 & -1/3 & 0 & -1/3 & 0 \\
-1/4 & 1 & 0 & -1/4 & -1/4 & -1/4 \\
-1/4 & 0 & 1 & -1/4 & -1/4 & -1/4 \\
0 & -1/3 & -1/3 & 1 & 0 & -1/3 \\
-1/4 & -1/4 & -1/4 & 0 & 1 & -1/4 \\
0 & -1/4 & -1/4 & -1/4 & -1/4 & 1
\end{bmatrix}
\end{array}
$$

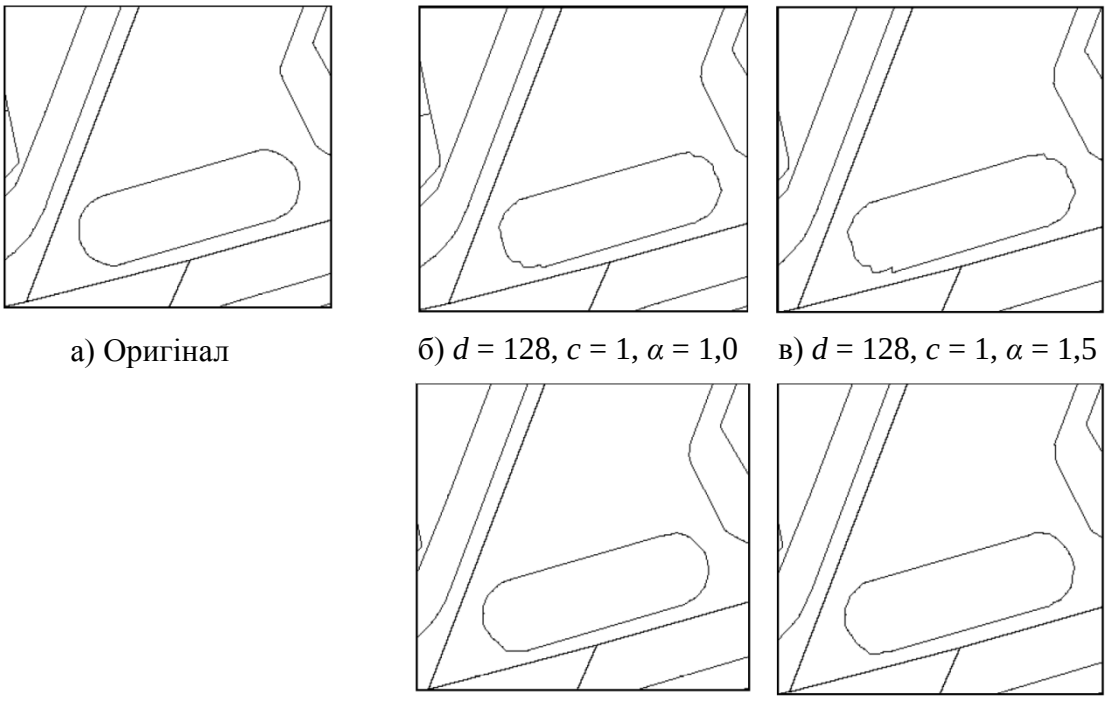
Рисунок 1.4 – Приклад сформованої матриці Лапласа частотних коефіцієнтів

Вбудовування бітів ЦВЗ проводиться шляхом зміни значень частотних коефіцієнтів залежно від біта ЦВЗ згідно з такою умовою:

$$b_i' = \begin{cases} -1, \textit{якщо } b_i = 0; \\ 1, \textit{якщо } b_i = 1. \end{cases} \quad (1.1)$$

Витягування ЦВЗ проводиться шляхом порівняння матриць частотних коефіцієнтів зображення з вбудованим ЦВЗ та матриць оригіналу векторного зображення.

Автори **запропонованого** методу проаналізували його щодо впливу вбудовування ЦВЗ на якість зображення, результати якого показані на рис. 1.5.



а) Оригінал

б) d = 128, c = 1, α = 1,0

в) d = 128, c = 1, α = 1,5

г) d = 480, c = 2, α = 1,0

д) d = 480, c = 3, α = 1,0

З вбудованими ЦВЗ

Рисунок 1.5 – Приклади фрагментів зображень до та після вбудовування ЦВЗ

ЛІТЕРАТУРА

1. Шелест М. Е. Введение в компьютерную стеганографию : монографія / В. А. Хорошко, М. Е. Шелест. — К., 2002. — 139 с.

2. Основи комп'ютерної стеганографії. Навчальний посібник / [В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук]. — Вінниця : ВДТУ. — 2003. — 143 с.

3. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

4. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : Солон-Пресс, 2002. — 272 с.

5. Трубей А. И. Обзор современных представлений о цифровой стеганографии / А. И. Трубей, М. Е. Шелест // Научно-технический журнал «Проблемы защиты информации». — Минск: БГУ. 2007. — № 3. — С. 515

6. Задірака В. К. Аналіз стійкості стеганографічних систем в моделі пасивного противника / В. К. Задірака, Н. В. Кошкіна, О. С. Олексюк // Искусственный интеллект. — 2004. — № 3. — С. 801—805.

7. Защита информации в телекоммуникационных системах / [Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов]. — К. : МК-Пресс, 2005. — 288 с.

8. Русин Б. П. Біометрична аутентифікація та криптографічний захист : монографія / Б. П. Русин, Я. Ю. Варецький; НАН України. Фіз.-мех. ін-т ім. Г. В. Карпенка. — Л. : Коло, 2007. — 287 с.

9. Кошкина Н. В. Анализ безопасности систем цифровых водяных знаков / Н. В. Кошкина // Компьют. математика: сб. науч. тр. — 2011. — Вып. 1. — С. 86—95. — Библиогр.: 15 назв. — рус.

10. Маракова И. И. Алгоритмы цифровых водяных знаков с точным восстановлением основных покрывающих сообщений / И. И. Маракова // Прав., нормат. та метрол. забезп. системи захисту інформації в Україні: наук.-техн. зб. — 2004. — Вип. 9. — С. 161—168.

11. Кобозева А. А. Анализ информационной безопасности : монографія / А. А. Кобозева, В. А. Хорошко. — К. : ГУИКТ, 2009. — 251 с.

12. 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.

13. Ohbuchi R. A shape-preserving data embedding algorithm for NURBS curves and surfaces / R. Ohbuchi, H. Masuda and M. Aono // Proc. Of Computer Graphics International'99[C], Canmore, Canada, 1999. — P. 170—177.

14. Sencar H. T. Data Hiding Fundamentals and Applications. / Husrev T. Sencar, Mahalingam Ramkumar, Ali N. Akansu. // Content Security İn Digital Multimedia Elsevier science and technology books, 2004. — 364 p.

15. Johnson N. F. İnformation Hiding: Steganography and Watermarking–Attacks and Countermeasures / Neil F. Johnson, Zoran Durič, Sushil Jajodia // Kluwer Academic Publishers, 2001. — 160 p.

16. Katzenbeisser S. İnformation Hiding Techniques for Steganography and Digital Watermark / Stefan Katzenbeisser, Fabien A. P. Petitcolas // Artech House Publishers, 1999. — 220 p.

17. Endoh U. Ueda and S. Endoh / U.Endoh // in the IEEE International Conference on Multimedia and Expo 2002[C], Lausanne, Switzerland, 2002. — P. 577—580.

18. Illustration watermarks for vector graphic / [H. Sonnet, T. Isenberg, J. Dittmann and T. Strothotte] // Proceedings of 11th Pacific Conference on Computer Graphics and Applications, Canmore, Canada, 2003. — P. 73—82.

19. Voigt M. Watermarking 2D-vector data for geographical information system / M. Voigt, C. Busch // Proceedings of IS&T/SPIE Electron Imaging[C], Washington, America, 2002. — № 4675. — P. 621—628.

20. Voigt M. Feature-based watermarking of 2D-vector data / M. Voigt and C. Busch. // Proceedings of SPIE[C], Santa Clara, 2003. — № 5020. — P. 359—366.

21. Schulz G. A high capacity watermarking system for digital maps / G. Schulz and M. Voigt // ACM Mutimedia and Security Workshop 2004[C], Magdeburg, Germany, 2004. — P. 180—186.

22. Lianquan M. The digital watermark of vector geo-data / Min Lianquan // Bulletin of Surveying and Mapping, 2007. — № 1. — P. 43—46.

23. Li Y. Copyright protection of the vector map using the digital watermark / Li Yuan-yuan and Xu Lu-ping // Journal of Xian University, 2004. — № 31(5). — P. 719—723.

24. Wang W. A robust watermarking algorithm for 2D vector graphics / Wang Wei and Li Ya // Journal of Image and Graphics. — № 12(2). — P. 200—205.

25. Shao C. Security issues of vector maps and a reversible authentication scheme / Shao Chengyong, Wang Xiaogong and Xu Xiaogang // Papers of 2005 Doctoral Forum of China, 2005. — P. 326—331.

26. Jia P. Technical methods for encrypting and hiding digital watermark in GIS spatial data / Jia Peihong, Ma Jinsong, Shi Zhaoliang and Xu Zhizhong // Geomatics and Information Science of Wuhan University, 2004. — № 29(8). — P. 747—750.

27. Ma T. Watermarking algorithm on 2D vector digital maps / Ma Tallin, Gu Chong and Zhang Liangpei // Geomatics and Information Science of Wuhan University, 2006. — № 31(9). — P. 192—294.

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

29. Tie-Sheng F. Method of vector graphics digital watermarking based on B-spline / Fan Tie-Sheng, Meng Yao and Fang Xiao-bing // Computer Engineering and Applications, 2007. — № 43(17). — P. 69—70.

30. Wang X. A robust watermarking algorithm for vector digital mapping / Wang Xun, Lin Hai and Bao Hujun // Journal of computer-aided design & computer Graphics, 2004. – № 16(10). – P. 1377–1381.

31. Chang-qing Z. An anticompression watermarking algorithm for vector map data / Zhu Chang-qing, Yang Cheng-song and Li zhong-yua // Journal of Zhengzhou Institute of Surveying and Mapping, 2006. – № 23(4). – P. 281–283.

32. Solachidis V. Watermarking polygonal lines using Fourier descriptors / V. Solachidis, N. Nikolaidis and I. Pitas. // Proc. of ICASSP'2000[C], Istanbul, Turkey, 2000. – P. 1955–1958.

33. V. Solachidis, N. Nikolaidis and I. Pitas. Fourier descriptors watermarking of vector graphics images, in the International Conference On Image Processing 2000[C], 2000. – № 3. – P. 9–12.

34. Giannoula A. Watermarking of sets of polygonal lines using fusion techniques / A. Giannoula, N. Nikolaidis and I. Pitas // IEEE International Conference on multimedia and Expro 2002[C], 2002. – P. 549–552.

35. Ohbuchi R.Watermarking 2D vector maps in the mesh-spectral domain / R. Ohbuchi, H. Ueda and S. Endoh // Fifth International Conference on Shape Modelling and Applications[C], Seoul, Korea, 2003. – P. 216–228.

36. Kitamura I. Copyright protection of vector map using digital watermarking method based on discrete Fourier transform / I. Kitamura, S. Kanai and T. Kishinami // in proceedings of IEEE 2001 International Geosciences and Remote Sensing[C], 2001. – P. 191–193.

37. Voigt M. Reversible watermarking of 2Dvector data / M. Voigt, B. Yang and C. Busch // in ACM Mutimedia and Security Workshop 2004[C], Magdeburg, Germany, 2004. – P. 160–165.

38. M. Voigt, B. Yang and C. Busch. High-capacity reversible watermarking for 2D-vectordata / M. Voigt, B. Yang and C. Busch // in Proceedings of the SPIE 2005[C], 2005. – № 5681. – P. 409–417.

39. Zhong Shang-ping. The feasibility analysis of normalized-correlation-based vector maps watermarking detection algorithm and the

improved watermarking algorithm / Zhong Shang-ping and Gao Qing-shi // in Journal of Image and Graphics, 2006. — № 11(3). — P. 401—409.

40. Yang Cheng-song. Watermarking algorithm for vector geo-spatial data based on wavelet transformation / Yang Cheng-song and Zhu Cang-qing // in Journal of Zhengzhou Institude of Surveving and Mapping, 2007. — № 24(1). — P. 37—39.

41. Li Yuanyuan. Vector graphical objects watermarking cheme in wavelet domain / Li Yuanyuan and Xu Luping // in Acta Photonica Sinica 2004. — № 1(33). — P. 97—100.

42. Zhang Qin. Watermarking vector graphics based on complex wavelet transform / Zhang Qin, Xiang Hui and Meng Xiang-xu // Journal of Image and Graphics, 2005. — № 4(10). — P. 12—15.

43. Kitamura I. Watermarking Vector digital map using wavelet transformation / I. Kitamura, S. Kanai and T. Kishinami // in Proceedings of Annual Conference of the Geographical Information Systems Association(GISA)[C], Tokyo, Japan, 2000. —P. 417—421.

44. Min Lianquan. A digital map watermarking algorithm based on discrete cosine transform / Min Lianquan and Yu Qihong // in Computer Applications and Software 2007. — № 24(1). — P. 146—148.

45. Mei ruirui. Copyright Protection of Digital Maps / Mei ruirui // Master's Degree Paper, Xian University, 2002.

46. Randall D. The digital dilemma[J] / D. Randall // Communications of the ACM, 2001. — Vol. 44(2). —P. 77—83.

47. Wei Huang. The Design of Image Digital Watermarking Based On the Human Vision System / Wei Huang // Master Dissertation, 2008.

48. Lianquan Min. A Robust Digital Watermarking in Cartographic Data in Vector Format / Lianquan Min // Mapping Bulletin, 2008. — Vol. 37(2). — P. 262—267.

49. Study on Adaptive Watermark of GIS Vector Data / [Lijuan Zhang, Li An-bo, Lv Guo-nian and Lin Bing-xian] // GEO-INFORMATION SCIENCE, 2008. — Vol. 10(6). — P. 724—728.

50. Xiangwei Zhu. Survey of Watermarking Performance Evaluation Indices on Digital Image / Xiangwei Zhu, Liang Xiao and Huizhong Wu // Communications Technology, 2009. — Vol. 42(91). P. 256—258.

51. Xiangwei Zhu. Robust of Still Image digital watermarking algorithm and performance evaluation methods / Xiangwei Zhu // Master Dissertation, 2007.

52. Zhengjiang. Research on Testing the Robustness of Digital Watermarking Algorithm / Zhengjiang Yi and Xiaoyan Zhou // Development and Application of Computer, 2009. —Vol. 22(5). P. 11—13.

53. Артёхин Б. В. Стеганография / Б. В. Артёхин // Защита информации. Конфидент. — 1996. — № 4. — С. 47—50.

54. Simmons G. J. The Prisoner's Problem and The Subliminal Channel / Gustavus J. Simmons / G. J. Simmons // Advances in Cryptology: Proceedings of Workshop on Communications Security CRYPTO'83. — New York : Plenum Press, 1984. — P. 51—67.

55. Pfitzmann B. İnformation Hiding Terminology / Birgit Pfitzmann // İnformation Hiding: Springer Lecture Notes in Computer Science. — Berlin: Springer-Verlag, 1996. — Vol. 1174. — P. 347—350.

56. Холл М. Комбинаторика / М. Холл. М. : Мир, 1970. — 424 с.

57. Baum C. W. Meteor Burst Communications / Carl W. Baum, Clint S. Wilkins // Wiley Encyclopedia of Electrical and Electronics Engineering. — New York : Wiley Publishing, 1999. — Vol. 12. — P. 592—596.

58. Nugent J. H. The İnformation Technology and Telecommunications (or E-Business) Security İmperative: İmportant İssues and Drivers / John H. Nugent, Mahesh S. Raisinghani // Journal of Electronic Commerce Research. — Long Beach : California State University, 2002. — Vol. 3, № 1. — P. 1—14.

59. Techniques for Data Hiding / [Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu] // İBM Systems Journal. — 1996. — Vol. 35, № 3, 4. — P. 313—336.

60. Cachin C. An İnformation-Theoretic Model for Steganography / Christian Cachin // İnformation Hiding, 2nd İnternational Workshop, Springer as Lecture Notes in Computing Science. — Berlin: Springer-Verlag, 1998. — Vol. 1525. — P. 306—318.

61. Kutter M. A Fair Benchmark For İmage Watermarking Systems / Martin Kutter, Fabien A. P. Petitcolas // Electronic İmaging'99: Security and Watermarking of Multimedia Contents, 25—27 Jan. 1999. — Vol. 3657. — P. 226—239.

62. Nunes P.R.R.L. Quality Measures of Compressed İmages for Classification Purposes. Technical Report CCR-146 / Paulo Roberto R. L. Nunes, Abraham Alcaim, Mara Regina da Silva. — Rio de Janeiro : İBM Brazil, Rio Scientific Center, 1992. — 48 p.

63. Oak Ridge National Laboratory's Cray XT5 «Jaguar» Supercomputer [Електронний ресурс]. — Режим доступу: http://www.cray.com/Products/XT5/ Product/ORNLJaguar.aspx.

64. Moulin P. İnformation-Theoretic Analysis of İnformation Hiding / Pierre Moulin, Joseph A. O'Sullivan // İEEE Transactions on İnformation Theory, March 2003. — Vol. 49. — № 3. — P. 563—593.

65. Su J. K. Analysis of Digital Watermarks Subjected to Optimum Linear Filtering and Additive Noise / Jonathan K. Su, Joachim J. Eggers, Bernd Girod // Signal Processing. Special İssue on İnformation Theoretic İssues in Digital Watermarking. — 2001. — Vol. 81. — № 6. — P. 1141—1175.

66. Marvel L.M. İmage Steganography for Hidden Communication: Ph.D Dissertation: Department of Computer and Electrical Engineering. / Lisa M. Marvel. — University of Delaware, 1999. — 115 p.

67. Ramkumar M. Data Hiding in Multimedia: Doctoral Thesis / Mahalingam Ramkumar. — Newark : New Jersey İnstitute of Technology, 1999. — 72 p.

68. Cox İ. J. Watermarking as Communications With Side İnformation / İngemar J. Cox, Matt L. Miller, Andrew L. McKellips // Proceedings of the İEEE. — 1999. — Vol. 87, № 7. — P. 1127—1141.

69. Evaluation framework of the effectiveness of image watermarking systems / [Daoshun Wang, Jinhong Liang, Dai Yi-qi et al.] // Journal of Computer Science and Technology, 2003. — Vol. 26(1). P. 779—788.

70. Shuqian Feng. Research on the Performance Testing Based on Digital Watermarking Algorithm / Shuqian Feng, Tihong Li // Software Guide, 2007. — P. 138—139.

71. Frank H. Spread spectrum watermarking: Malicious attacks and counterattacks[J] / H. Frank, K. S. Jonathan, G. Bernd // Proceedings of the SPIE-The International Society for Optical Engineering, 1999. — P. 147—148.

72. A survey on attacks in image and video watermarking[J] / [Boris V, Philippe N, Severine B et al.] // Proceedings of the SPIE-The International Society for Optical Engineering, 2002. — P. 169—179.

73. Digital watermarking[M] / [Ingamar. J Cox, Matthew L. Miller, Jeffrey A. Bloom] // Morgan Kaufmann, 2002.

74. Anbo Li. Research on Key technique for Copyright Protecting of GIS Vector Data / Anbo Li // Doctorial Dissertation, 2007.

75. Digital Watermarking Technology and its Application / [Shenghe Sun, Zheming Lu, NiuXia-mu et al.]. — 2003.

76. Hongbin Zhang. A Review of Watermarking Application, their Properties and Benchmarking / Hongbin Zhang, Fan Zhang // Computer Science, 2003. Vol. 30 (8). P. 59—63.

77. Geographic Information System Arithmetic Fundamentals / [Hong Zhang, Yongning Weng, Aili Liu et al.]. — 2006.

78. Zhiqiang Wu. Application and Benchmark Test Software of Image Digital Watermarking / Zhiqiang Wu // Journal of East China Jiao tong University, 2004. — Vol. 21 (1). P. 98—102.

79. Яремчук Ю. Є. Про захист авторського права в зображеннях за допомогою цифрових водяних знаків / Ю. Є. Яремчук, В. В. Карпінець // Тези доповідей II Міжнародної науково-технічної конференції «Сучасні інформаційно-комунікаційні технології». — К. : Вісник. — 2006. — С. 17.

80. Яремчук Ю. Є. Метод приховування інформації в зображеннях на основі специфічних особливостей формату файла / Ю. Є. Яремчук,

В. В. Карпінець // Збірка тез доповідей учасників IV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Технології безпеки інформації». — К. : 2006. — С. 15.

81. Яремчук Ю. Є. Карпінець В.В. Про один метод приховування інформації в зображеннях / Ю. Є. Яремчук, В. В. Карпінець // Тези доповідей четвертої науково-технічної конференції «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – К. : ПП «ЕКМО». — 2006. — С. 79.

82. Карпінець В. В. Приховування інформації на основі специфічних особливостей файлів / Карпінець В. В. // Тези студентських доповідей XXXV науково-технічної конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та галузі. — Вінниця : УНІВЕРСУМ-Вінниця. — 2006. — С. 52.

83. Яремчук Ю. Є. Використання цифрових водяних знаків для захисту авторського права в зображеннях / Ю. Є.Яремчук, В. В. Карпінець // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні. — 2006. — № 2(13). — С. 63—69.

84. Свідоцтво про реєстрацію авторського права на твір № 17207. Комп'ютерна програма «Програма для приховування інформації в JPEG-файлах» / Ю. Є. Яремчук, В. В. Карпінець — К. : Державний департамент інтелектуальної власності України. Дата реєстрації: 11.07.06.

85. Яремчук Ю. Є. Аналіз стійкості стеганографічного перетворення до вбудовування цифрових водяних знаків у зображення / Ю. Є. Яремчук, В. В. Карпінець // Інформаційні технології та комп'ютерна інженерія. — 2007. — № 1(8). — С. 212—217.

86. Яремчук Ю. Є. Вирішення задачі забезпечення захисту авторського права в зображеннях / Ю. Є. Яремчук, В. В. Карпінець // Матеріали V науково-технічної конференції студентства та молоді «Світ інформації та телекомунікацій – 2008». — 2008. — С. 28—29.

87. Яремчук Ю. Є. Використання цифрових водяних знаків для захисту авторського права в зображеннях / Ю. Є. Яремчук, В. В. Карпінець // Тези доповідей ІІІ Міжнародної науково-технічної конференції «Сучасні інформаційно-комунікаційні технології». — К. : Вісник. — 2007. — С. 266.

88. Яремчук Ю. Є. Підвищення стійкості цифрових водяних знаків до спотворення зображень / Ю. Є. Яремчук, В. В. Карпінець // Збірка тез доповідей VI всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». — 2008. — С. 143—144.

89. Яремчук Ю. Є. Вирішення проблеми захисту авторського права у цифрових зображеннях / Ю. Є. Яремчук, В. В. Карпінець // Збірник матеріалів шостої міжнародної конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2008». — С. 419—420.

90. Яремчук Ю. Є. Проблеми захисту авторського права растрових та векторних зображень / Ю. Є. Яремчук, В. В. Карпінець // Збірник тез VII науково-технічної конференції «Світ інформації та телекомунікацій – 2010». — К. : ДУІКТ, 2010. — С. 169—170.

91. Яремчук Ю. Є. Аналіз методів вбудовування цифрових водяних знаків у векторні зображення / Ю. Є. Яремчук, В. В. Карпінець // Збірник матеріалів шостої міжнародної конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2010». — С. 408—409.

92. Яремчук Ю. Є. Проблеми стеганографічного захисту векторних зображень / Ю. Є. Яремчук, В. В. Карпінець // Тези доповідей XIII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах». — К., 2010. —С. 62—63.

93. Яремчук Ю. Є. Захист векторних зображень цифровими водяними знаками / Ю. Є. Яремчук, В. В. Карпінець // Збірка тез доповідей IX всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 2011. —С. 109—110.

94. Яремчук Ю. Є. Зменшення впливу цифрових водяних знаків на векторні зображення при їх вбудовуванні / Ю. Є. Яремчук, В. В. Карпі-

нець // Тези доповідей XIV міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах». —К., 2011. —С. 80—81.

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

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

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

98. Яремчук Ю. Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних Ю. Є. Яремчук, В. В. Карпінець // Сучасний захист інформації. —2011. —№ 2. — С. 94—99 .

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

100. Яремчук Ю. Є. Аналіз стійкості методу вбудовування цифрових водяних знаків у векторні зображення до зловмисних атак / Ю. Є. Яремчук, В. В. Карпінець // Вісник Вінницького політехнічного інституту. — 2011. —№ 4. —С. 154—159.

101. Яремчук Ю. Є. Метод захисту авторського права в зображеннях формату Jpeg за допомогою цифрових водяних знаків / Ю. Є. Яремчук, В. В. Карпінець // Вісник ДУІКТ. —2006. —№ 4(3). —С. 206—211.

102. Яремчук Ю. Є. Приховування інформації в зображеннях на основі специфічних особливостей формату файла / Ю. Є. Яремчук, В. В. Карпінець // Захист інформації. −2006. −№ 2(29). −С. 24−29.

103. Патент на корисну модель №57243, (51) МПК (2011) H03M 13/37. Спосіб захисту авторських прав векторних зображень цифровими водяними Ю. Є. Яремчук, В. В. Карпінець. −№ u2010 15193; заявл. 16.12.2010; опубл. 10.02.2011; Бюл. № 3, 2011.

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

105. Дьяконов В. П. Энциклопедия MathCAD 2001i и MathCad 11 / В. П. Дьяконов. − М. : Солон-Пресс, 2004. − 464 с.

106. Свідоцтво про реєстрацію авторського права на твір №39748 Комп'ютерна програма «Комп'ютерна програма для вбудовування цифрових водяних знаків у цифрові зображення векторного формату» / Ю. Є. Яремчук, В. В. Карпінець. − К. : Державний департамент інтелектуальної власності України. Дата реєстрації: 18.08.11.

Наукове видання

Карпінець Василь Васильович
Яремчук Юрій Євгенович

МЕТОДИ ЗАХИСТУ ВЕКТОРНИХ ЗОБРАЖЕНЬ ЦИФРОВИМИ ВОДЯНИМИ ЗНАКАМИ

Монографія

Редактор Н. Мазур

Оригінал-макет підготовлено В. Карпінцем

Підписано до друку 21.03.2013 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. др. арк. 14,32
Наклад 300 (1-й запуск 1–75) Зам № 2013-071

Вінницький національний технічний університет,
КІВЦ ВНТУ,
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-85-32.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті,
в комп'ютерному інформаційно-видавничому центрі,
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-81-59
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.