УДК 004.056.5

к.т.н. **Ахмаметьєва Г.В.** (ОНПУ)
Баранюк Г.А. (ОНПУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-03

РОЗРОБКА СИСТЕМИ ВБУДОВИ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В ЗОБРАЖЕННЯ НА ОСНОВІ DCT-LWT-SVD

Захист авторського права на цифровий контент – досить актуальна проблема людства у XXI столітті, оскільки випадки неправомірного використання мультимедійного контенту спостерігаються дуже часто, і їх кількість постійно зростає. Одним із видів захисту авторської власності є вбудовування цифрового водяного знаку (ЦВЗ) у контент.

У роботі запропоновано новий метод вбудовування цифрового водяного знаку у зображення-контейнер з використанням дискретного косинусного перетворення (DCT), ліфтингового вейвлет-перетворення (LWT) з материнським вейвлетом «Добеші-8» та сингулярного розкладу матриці (SVD). Вбудовування здійснюється у перше сингулярне число, отримане сингулярним розкладанням області низьких частот вейвлет-перетворення. В якості цифрового водяного знаку використовуємо полутонове зображення, нормоване в діапазон від нуля до десяти для забезпечення високого показника пікового відношення сигнал/шум (PSNR).

В дослідженні проведено аналіз розробленого методу: алгоритмічна реалізація вбудовування та детектування інформації перевірена на стійкість до різних видів атак, а саме: накладання шумів (Гаусів та мультиплікативний шуми, «сіль та перець»), застосування фільтру «unsharp» та медіанного фільтру, атака стисненням (з коефіцієнтами якості для заповненого контейнеру від 60 до 100). В результаті проведеного тестування, встановлено, що метод є досить стійким до усіх аналізованих атак, окрім фільтрації «unsharp» (результуючі показники не є задовільними).

Метод показав гарні результати по піковому відношенню сигнал/шум – середнє значення PSNR дорівнює 50,5 дБ, а також високі показники вилучення вбудованого ЦВЗ – точність детектування складає від 77% до 97,6 % при збереженні заповненого контейнеру у форматі без втрат.

Ключові слова: стеганографія, цифровий водяний знак, дискретне косинусне перетворення, ліфтингове вейвлет-перетворення, сингулярне розкладання матриць, цифрове зображення.

Вступ та аналіз останніх досліджень. У наш час – вік цифрових технологій – інформація має певну ціну та цінність, тому з кожним моментом часу конфіденційна та таємна інформація знаходиться у зоні ризику. Ризики являють собою ряд факторів, що будуть впливати на властивості захищених даних. Одним з таких ризиків є отримання зловмисником або порушником незаконним шляхом необхідної інформації. Особливо цікавим є питання захисту авторського права цифрових даних. Саме тому у сфері інформаційних технологій було створено такий вид захисту інформації як цифровий водяний знак.

Цифровий водяний знак - це сигнал, що є вбудованим на постійній основі у цифрові дані (аудіо, зображення, відео та текст), який можна виявити або витягти за допомогою обчислювальних операцій для підтвердження їх наявності. ЦВЗ - це спеціальна мітка, вбудована в цифровий контент з метою захисту авторських прав і підтвердження цілісності самого документа. ЦВЗ приховується у даних контейнеру таким чином, що він стає невіддільним від них, цим самим забезпечуючи стійкість до багатьох операцій, що не погіршують контейнер [1].

Останнім часом дослідження в області цифрових водяних знаків, порівняно із іншими напрямами, стрімко зростають, адже тема захисту секретної/конфіденційної інформації стає дедалі актуальнішою. З кожним роком кількість робіт, присвячених даній темі збільшується, а методи, що існували до сьогоднішнього дня – вдосконалюються.

Серед стеганографічних методів вбудови інформації в область ДКП можна виділити роботи [2-4]. В роботах [2, 3] забезпечується висока пропускна здатність прихованого каналу зв'язку, однак візуальна цілісність заповненого контейнеру досить низька – показник пікового відношення сигнал/шум (PSNR) складає від 33 до 40 дБ. В роботі [4] навпаки забезпечуються

високі значення PSNR (від 55 до 68 дБ) за рахунок вбудови повідомлення малої довжини, що декілька обмежує область застосування запропонованого методу, особливо за необхідності вбудувати текст значного об'єму або ЦВЗ-зображення.

Щодо області вейвлет-перетворення, слід відрекомендувати роботи [5-6]. Ці алгоритми забезпечують високий рівень PSNR та об'єм інформації, що можна передати, проте головним їх недоліком є складність реалізації. Крім того, в роботі [5], незважаючи на високу стійкість до атак, пропонується система ЦВЗ напівзакритого типу [1], що не передбачає вилучення ЦВЗ.

Стаття [7] порівнює показники спотворень у заповнених контейнерах в порівнянні з оригінальним та вилучення ЦВЗ при використанні методів на основі DCT і DWT-перетворень, де перевага надається методу на основі дискретного косинусного перетворення.

Розглядаючи методи [8-12], у яких йде мова про спільне використання дискретного косинусного та дискретного вейвлет-перетворень, необхідно акцентувати на тому, що застосування цих двох перетворень в комплексі дають кращі результати, аніж їх використання окремо.

Статті [8-10] присвячені розробці закритих систем ЦВЗ, для яких характерним є використання оригінального контейнеру для вилучення ЦВЗ. В роботі [8] запропоновано систему ЦВЗ з використанням дискретного косинусного перетворення (DCT – Discrete Cosine Transform), дискретного вейвлет-перетворення (DWT – Discrete Wavelet Transform) та сингулярного розкладу матриць (SVD – Singular Value Decomposition), що дозволило отримати значення PSNR близько 52 дБ. Стаття [9] використовує комбінацію DWT і DCT-перетворень для вбудови бінарного ЦВЗ-зображення. При високих показниках PSNR та стійкості до атак візуально спостерігається посилення контрасту заповненого контейнера в порівнянні з оригіналом, що підкреслює наявність ЦВЗ в зображенні або його обробку.

В статті [11] запропонований стійкий до атак метод вбудови ЦВЗ на основі DWT-DCT-перетворень. При малих значеннях пропускної здатності забезпечуються високі показники PSNR, однак точність вилучення ЦВЗ досить низька. Однак при збільшенні об'єму повідомлення зростає точність детектування, але порівняння пустого і заповненого контейнерів дає значення PSNR с середньому 45 дБ. Робота [12] пропонує використання комбінації DWT-DCT-SVD-перетворень для методу, стійкого до атак. Однак основним недоліком методу є низькі значення PSNR (від 32 до 41 дБ).

Отже, аналіз досліджень, присвячених захисту зображень за допомогою ЦВЗ, виявив ряд протиріч між візуальною цілісністю заповнених контейнерів і точністю вилучення вбудованого ЦВЗ. Тому метою роботи є розробка методу вбудови ЦВЗ в зображення, що забезпечує високу якість заповненого контейнеру.

Основна частина. В якості контейнеру будемо використовувати кольорове цифрове зображення (ЦЗ), представлене в схемі RGB. Цифровий водяний знак представляє собою полутонове зображення або кольорове зображення, перетворене в ЦЗ в градаціях сірого. Значення яскравості ЦВЗ в діапазоні $[0,255]$ нормуються в діапазон $[0,10]$ у відповідності з формулою:

$$M' = \frac{M}{255} \cdot 10, \tag{1}$$

де M – полутонове зображення ЦВЗ, M' – нормований ЦВЗ.

Для методу, що розробляється, будемо використовувати поетапне застосування дискретного косинусного перетворення, ліфтінгового вейвлет-перетворення (LWT) та сингулярного розкладу матриці подібно методу [8], але на відміну від запропонованої в [8] системи вилучення ЦВЗ реалізується «в сліпу», тобто без використання оригінального контейнеру.

Вбудова інформації здійснюється наступним чином. Матриця контейнера поділяється на блоки 8×8, що не перетинаються. До кожного блоку застосовується дискретне косинусне перетворення. Для матриці отриманих коефіцієнтів DCT обчислюється ліфтингове вейвлет-перетворення. В свою чергу до матриці низьких частот (LL) застосовується сингулярний

розклад та виділяються сингулярні числа. В один блок матриці контейнеру можна помістити один елемент ЦВЗ. Процес вбудовування ЦВЗ здійснюється перше сингулярне число у відповідності з формулою:

$$s_1' = \begin{cases} \lfloor s_1/10 \rfloor + m', & s_1 \geq 20, \\ 1.8m', & m' \geq 5, \\ m' + 4, & m' < 5, \end{cases} \quad (2)$$

де s_1 – значення першого сингулярного числа (СНЧ), s_1' – модифіковане значення першого СНЧ, $m', m' \in M'$ – нормоване значення яскравості ЦВЗ.

Аналіз сингулярних чисел матриці низьких частот LWT-перетворення показав, що в більшості випадків друге, третє і четверте сингулярні числа найбільш схильні до округлень. Тому для вбудови використовується перше СНЧ. При цьому значення m' поділяються на два піддіапазони: $[0,5)$ і $[5,10]$, до яких застосовуються різні формули модифікації першого СНЧ (2). В результаті піддіаназон m' $[0,5)$ дає значення першого СНЧ, що належать $[0,9)$, а піддіапазон $[5,10]$ - значення першого СНЧ, що належать $[9,18]$.

Вилучення ЦВЗ з заповненого контейнеру відбувається аналогічними послідовними DCT-LWT-SVD-перетвореннями блоків 8×8 за формулою:

$$w = \begin{cases} s_1' - \lfloor s_1'/10 \rfloor \cdot 10, & s_1' \geq 20, \\ s_1'/1.8, & s_1' \geq 9, \\ s_1' - 4, & s_1' < 9, \end{cases} \quad (3)$$

після чого отримане значення повертається в діапазон $[0,255]$:

$$w = \left\lfloor \frac{w}{10} \cdot 255 \right\rfloor, \quad (4)$$

де w – детектований ЦВЗ, s_1' – перше сингулярне число SVD-розкладання матриці низьких частот LWT-перетворення DCT-коефіцієнтів блоку заповненого контейнеру, $\lfloor \ldots \rfloor$ - операція округлення до найближчого цілого.

В ході експериментального тестування вбудови і вилучення ЦВЗ при використанні різних колірних складових контейнеру помічено, що результати вилучення ЦВЗ різні: в одному випадку спостерігається мінімальна кількість помилок з точки зору візуальної цілісності ЦВЗ, в інших – значні візуально помітні спотворення, аналіз яких буде проведено нижче.

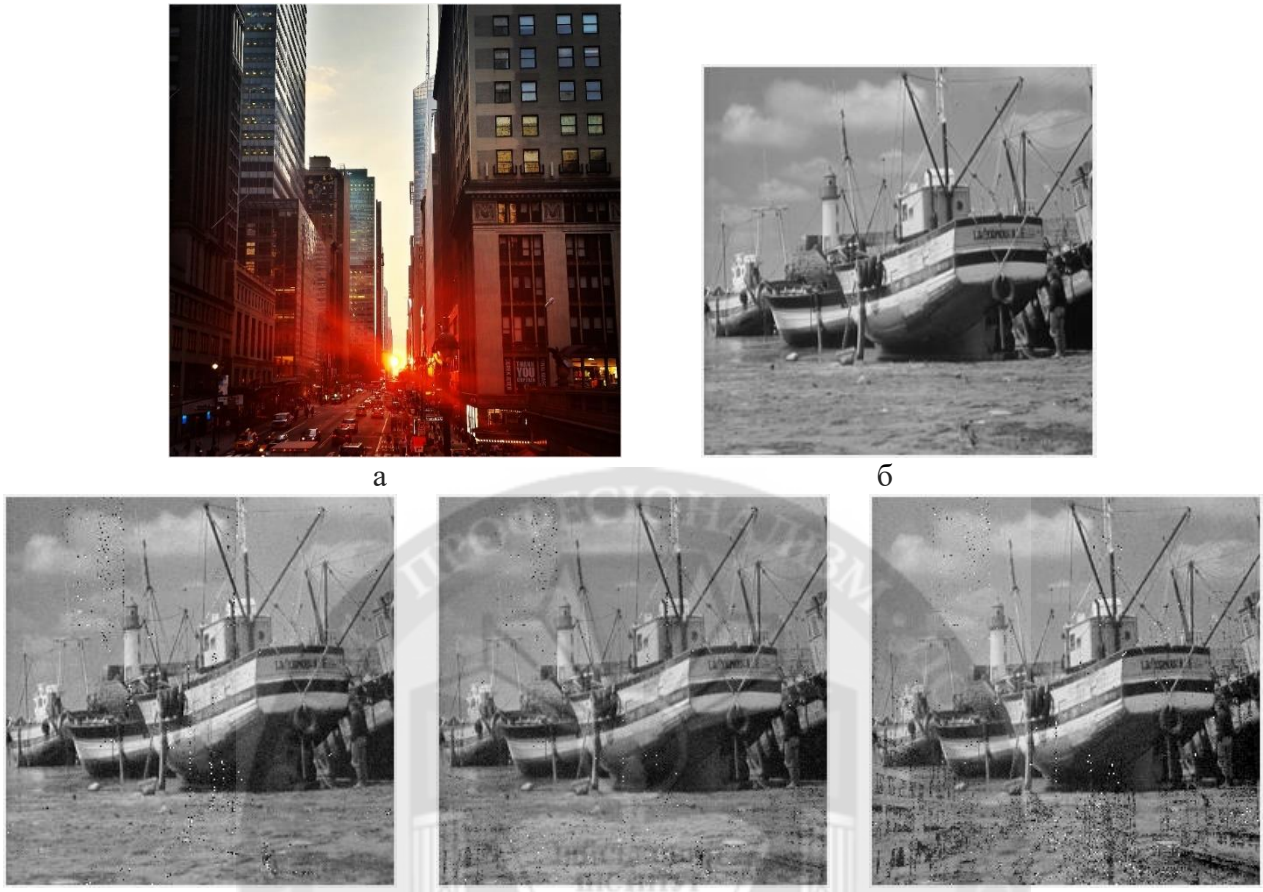
Слід зазначити, що у зв'язку з вбудовою ЦВЗ в область перетворень, яка передбачає округлення коефіцієнтів як DCT-перетворення, так і LWT-перетворення і сингулярного розкладання, а також представлення ЦВЗ в діапазоні $[0,10]$, визначення точності вилучення ЦВЗ стандартними показниками, що аналізують бітову послідовність, такими як NCC [13], SIM [7], BCR [11] може дати незадовільні результати, оскільки значення яскравості оригінального і вилученого ЦВЗ можуть відрізнятися на 5-10 одиниць, що призведе до низьких значень зазначених показників при збереженні візуальної цілісності вилученого ЦВЗ. У зв'язку з цим точність вилучення вбудованого ЦВЗ будемо оцінювати ступенем подібності, що визначається за наступним алгоритмом.

Обчислення ступеню подібності вбудованого і вилученого ЦВЗ.

Крок 1. Якщо $\left| m_{i,j} - m'_{i,j} \right| \leq 10$, то $count = count + 1$, де $m_{i,j}, m'_{i,j}$ - значення яскравості вбудованого і вилученого ЦВЗ відповідно, $i = \overline{1,H}$, $j = \overline{1,W}$, $H \times W$ - розмір ЦВЗ.

Крок 2. Обчислити $SD = \dfrac{count}{H \cdot W}$.

На рис. 1 наведено приклад вбудовування ЦВЗ (рис.1, б) в контейнер (рис.1, а) лише в червону, зелену та синю колірні складові. Результати вилучення ЦВЗ наведені на рис.1, в-д.



а б в г д

Рисунок 1 – Результати детектування ЦВЗ: а – контейнер розміром 2048×2048; б – оригінальний ЦВЗ розміром 256×256; в – ЦВЗ, вилучений з червоної колірної складової (SD=0.9408, NCC=0.3788, SIM=0.6724, BCR=0.6894); г – ЦВЗ, вилучений з зеленої колірної складової (SD=0.9142, NCC=0.3651, SIM=0.6657, BCR=0.6825); д – ЦВЗ, вилучений з синьої колірної складової (SD=0.8205, NCC=0.3270, SIM=0.6438, BCR=0.6635)

Як видно з рис. 1, навіть при деяких спотвореннях ЦВЗ зберігається його візуальна цілісність, проте показники NCC, SIM і BCR дають низькі значення, крім того найбільші спотворення характерні для ЦВЗ, вилученого з синьої колірної складової.

Аналіз причин помилок при вилученні ЦВЗ показав, що в більшості випадків некоректне детектування значень ЦВЗ відбувається в блоках, які містять більшість значень, що прагнуть до 0 або 255. У зв'язку з чим запропоновано наступний алгоритм для визначення колірної складової, найбільш придатної для вбудови ЦВЗ.

Вибір колірної складової зображення для вбудови/вилучення ЦВЗ.

Крок 1. Розбити колірну складову I^y, $y\in\{R,G,B\}$ розміром $M\times N$ цифрового зображення на блоки B^y розміром 8×8, що не перетинаються.

Крок 2. Для кожного блоку B^y:

2.1. Обчислити $R=\sum_{i,j=1}^{8} b_{i,j} \Big/ (255\cdot64)$.

2.2. Якщо $R<0.1$, то $E_1^y=E_1^y+1$, де E_1^y - кількість блоків зі значеннями яскравості, що наближаються до 0, y-ої колірної складової.

2.3. Якщо $R > 0.9$, то $E_2^y = E_2^y + 1$, де E_2^y - кількість блоків зі значеннями яскравості, що наближаються до 255, y -ої колірної складової.

Крок 3. Обчислити $P^y = \left(E_1^y + E_2^y\right) / k$, де $k = \left\lfloor \frac{M}{8} \right\rfloor \cdot \left\lfloor \frac{N}{8} \right\rfloor$ - кількість блоків 8×8 колірної складової I^y, $\lfloor \ldots \rfloor$ - округлення до меншого цілого.

Крок 4. Для вбудови/вилучення ЦВЗ обирається колірна складова з мінімальним значенням P.

Необхідно акцентувати увагу на вейвлет-функції, що використовується в при обчисленні LWT-перетворення. В результаті проведення чисельних експериментів, було визначено, що найефективнішими материнськими вейвлетами є функції «Добеші-8» та «Хаара». Однак при використанні вейвлету «Хаара» спотворення ЦВЗ є більш помітними, тому найоптимальнішим варіантом є використання вейвлету «Добеші-8».

З урахуванням проведених експериментів сформулюємо основні кроки системи ЦВЗ.

Вбудова ЦВЗ в контейнер.

Крок 1. Визначити колірну складову для вбудови ЦВЗ.

Крок 2. Нормалізувати ЦВЗ у відповідності з формулою (1).

Крок 3. Обрану колірну складову ЦЗ I розміром $M \times N$ розбити на блоки B розміром 8×8, що не перетинаються.

Для кожного блоку B (кроки 4-10):

Крок 4. Виконати дискретне косинусне перетворення. Результат - B_{dct}.

Крок 5. До коефіцієнтів DCT B_{dct} застосувати ліфтінгове вейвлет перетворення. Результат – матриці LL, LH, HL, HH розміром 4×4.

Крок 6. Для матриці LL виконати сингулярне розкладання. Результат - S - матриця СНЧ, U, V - матриці сингулярних векторів.

Крок 7. Замінити перше СНЧ у відповідності з формулою (2).

Крок 8. Відновити матрицю низьких частот LL': $LL' = U \cdot S' \cdot V$, де S' - модифікована матриця СНЧ.

Крок 9. Застосувати обернене ліфтінгове вейвлет перетворення. Результат - $B_{dct}{}'$.

Крок 10. Виконати обернене дискретне косинусне перетворення. Результат - B'.

Крок 11. Зберегти заповнений контейнер.

Вилучення ЦВЗ з заповненого контейнеру.

Крок 1. Визначити колірну складову для вбудови ЦВЗ.

Крок 2. Обрану колірну складову ЦЗ I' розміром $M \times N$ розбити на блоки B' розміром 8×8, що не перетинаються.

Для кожного блоку B' (кроки 3-7):

Крок 3. Виконати дискретне косинусне перетворення. Результат - $B_{dct}{}'$.

Крок 4. До коефіцієнтів DCT $B_{dct}{}'$ застосувати ліфтінгове вейвлет перетворення. Результат – матриці LL', LH', HL', HH' розміром 4×4.

Крок 5. Для матриці LL' виконати сингулярне розкладання. Результат - S' - матриця СНЧ, U', V' - матриці сингулярних векторів.

Крок 6. Обчислити нормалізоване значення ЦВЗ у відповідності з формулою (3).

Крок 7. Перевести нормалізоване значення до діапазону $[0, 255]$ у відповідності з формулою (4).

Крок 8. З отриманих значень яскравості сформувати ЦВЗ.

Для оцінки ефективності запропонованого методу був проведений обчислювальний експеримент на основі 200 кольорових ЦЗ при використанні різних ЦВЗ. Ефективність стеганографічного методу будемо оцінювати визначенням показника PSNR, порівнюючи оригінальний і заповнений контейнери, та ступенем подібності вилученого ЦВЗ та вбудованого ЦВЗ. До заповнених контейнерів були накладені певні атаки, такі як зашумлення, підвищення різкості і медіанна фільтрація. В даному експерименті заповнені контейнери були збережені в форматі без втрат. Результати обчислювального експерименту наведені в табл. 1.

Таблиця 1

Ефективність вилучення ЦВЗ із заповненого контейнеру

Атака	Параметр	Середнє значення PSNR, дБ	Середнє значення ступеню подібності, %
Без атаки		50.45	93.85
Гаусів шум	$m = 0.0001$, $d = 0.0000005$	48.67	93.44
	$m = 0.001$, $d = 0.00005$	50.40	81.86
Мультиплікативний шум	$d = 0.0001$	50.45	81.76
	$d = 0.00001$	41.96	85.73
	$d = 0.000001$	48.62	93.72
Шум «Сіль та перець»	$d = 0.0001$	44.01	93.50
Фільтр підвищення різкості «Unsharp»		41.79	35.20
Медіанний фільтр		39.50	50.47

З табл. 1 видно, що запропонований метод забезпечує високі значення PSNR при збереженні заповненого контейнера в форматі без втрат – значення коливаються в межах 45 дБ до 56 дБ при забезпеченні високої пропускної здатності прихованого каналу зв'язку, що перевищує результати існуючих аналогів. Також метод є стійким до зашумлення – середні значення ступеню подібності перевищують 80%, причому у всіх зображень мінімальні значення ступеню подібності не нижче 70%. Однак запропонований метод виявився нестійким до медіанної фільтрації і підвищення різкості.

В табл. 2 наведені результати вилучення ЦВЗ з заповненого контейнеру, що зазнав атаку JPEG-стисненням.

Таблиця 2

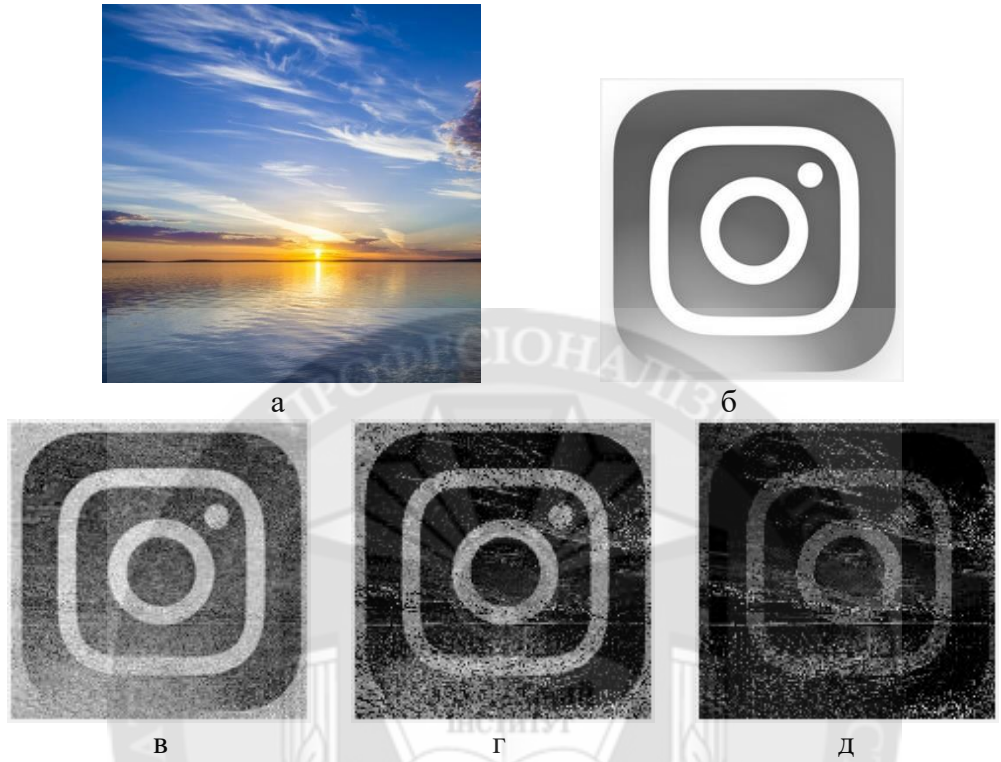
Ефективність вилучення ЦВЗ із заповненого контейнеру після JPEG-стиснення

Показник якості		*QF*								
		60	65	70	75	80	85	90	95	100
Середнє значення PSNR, дБ		38.86	40.72	42.93	47.93	44.47	43.64	45.99	47.07	47.77
	Подібність ЦВЗ									
Ступень подібності, %	Максимальне значення	87.50	89.16	88.14	88.90	87.88	87.76	87.76	89.16	91.96
	Мінімальне значення	1.78	1.89	1.80	2.15	2.49	2.53	1.57	1.46	2.24
	Середнє значення	28.88	26.76	26.78	24.06	25.01	26.65	27.90	29.22	34.23

З табл. 2 видно, що стиснення значно погіршує показники подібності вбудованого та вилученого ЦВЗ, які охоплюють широкий діапазон значень від 1,5% до 90%, причому тільки в 26% заповнених контейнерів при стисненні з $QF = 100$ ступень подібності перевищує 50%.

Однак, незважаючи на погіршення показників при стисненні, вилучений ЦВЗ залишається візуально помітним і зберігає можливість визначення авторства.

На рис. 2 наведений оригінальний ЦВЗ (рис. 2, б), вбудований в контейнер (рис. 2, а), та ЦВЗ, вилучені з заповнених контейнерів після атаки стиском (рис. 2, в-д). Незважаючи на наявність шумів, що повторюють контури контейнера і зростають зі зменшенням QF, цифровий водяний знак можна ідентифікувати при $QF \geq 80$.



а б в г д

Рисунок 2 – Результати детектування ЦВЗ після атаки стисненням: а – контейнер розміром 1200×1200; б – оригінальний ЦВЗ розміром 150×150; в – вилучений ЦВЗ зі стиснутого з $QF = 100$ заповненого контейнеру(SD=15.72%); г – вилучений ЦВЗ зі стиснутого з $QF = 90$ заповненого контейнеру(SD=1.88%); д – вилучений ЦВЗ зі стиснутого з $QF = 80$ заповненого контейнеру(SD=1.52%)

Висновки. В роботі розроблений новий метод вбудовування цифрового водяного знаку у зображення з послідовним використанням DCT-LWT-SVD-перетворень. Перед вбудовою ЦВЗ зображення-контейнер аналізується для вибору колірної складової, найбільш придатної для вбудови додаткової інформації, що веде до мінімізації помилок вилучення ЦВЗ.

В результаті проведених обчислюваних експериментів, спрямованих на визначення якості отриманих заповнених контейнерів, а також їх стійкості до атак, встановлено, що забезпечуються високі значення PSNR, які в середньому складають 50.45 дБ, при збереженні високої пропускної здатності прихованого каналу зв'язку. Експериментально доказана стійкість запропонованого методу до атак, зокрема до зашумлення зображення та стиснення ЦЗ при $QF \geq 80$. При накладанні шумів зберігається висока ступень подібності між оригінальним і вилученим ЦВЗ. У випадку стиснення ЦЗ при досить низьких значеннях ступеню подібності вилучений ЦВЗ піддається ідентифікації.

ЛІТЕРАТУРА:

1. Грибунин, В.Г. Цифровая стеганография / В. Грибунин, И. Оков, И. Туринцев. – Москва. : СОЛОН-Пресс, 2017. -262 с.

2. Senthooran V. DCT Coefficient Dependent Quantization Table. Modification Steganographic Algorithm / V.Senthooran, L.Ranathunga // First International Conference on Networks & Soft Computing. – 2014. – С. 432-436.

3. Alwan I. Image Hiding Using Discrete Cosine Transform / I. Alwan, F. Mohammed // J. Of College Of Education For Women. – 2016. - №27. – С. 393-399.

4. Nagpal C. Modified quantization based steganography for color images / C. NAGPAL, R. GOEL // International Journal of Electrical and Electronics Engineering. – 2013. - №2. – С. 9-17.

5. Ахмаметьєва Г. Модифікація стеганографічного методу вбудови цифрового водяного знаку в зображення на основі вейвлет-перетворення / Г.В. Ахмаметьєва, Г.А. Баранюк // Інформатика та мамематичні методи в моделюванні. – 2019. - №1. – С. 76-87.

6. Singh B. Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR / B. Singh // International Journal of Emerging Research in Management &Technology. – 2017. - №8. – С. 230-234.

7. Jabbar K. Compare Between DCT and DWT for Digital Watermarking in Color Image / K. Jabbar, B. Tuieb // Information and Knowledge Management. – 2015. - №5(7). – С. 22-31.

8. Singh N. High PSNR based Image Steganography / N. Singh // International Journal of Advanced Engineering Research and Science. – 2019. - №1. – С. 109-115.

9. Al-Haj A. Combined DWT-DCT Digital Image Watermarking / A. Al-Haj // Journal of Computer Science. – 2007. - №3(9). – С. 740-746.

10. Akter A. Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm / A. Akter, N. Tajnina, M. International Conference on Informatics, Electronics & Vision (ICIEV). – 2014. - № 10. – С. 1-6.

11. Benoraira A. Blind image watermarking technique based on differential embedding in DWT and DCT domains / A. Benoraira, K. Benmahammed, N. Boucenna // Benoraira et al. EURASIP Journal on Advances in Signal Processing. – 2017. - №55. – С. 1-11.

12. Rahman M. A DWT, DCT AND SVD BASED WATERMARKING TECHNIQUE TO PROTECT THE IMAGE PIRACY / M. Rahman // International Journal of Managing Public Sector Information and Communication Technologies. – 2013. - №4(2). – С. 1-12.

13. Мельник, М.А. Методика оценки устойчивости стеганоалгоритма к сжатию / М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. - 2013. - Вип. 44. - С. 121-128.

REFERENCES:

1. Gribunin V.G. (2017), “Cyfrovaya steganographiya” [Digital steganography], SOLON-Pres, 262 p.

2. Senthooran V., Ranathunga L. (2014), “DCT Coefficient Dependent Quantization Table. Modification Steganographic Algorithm”, First International Conference on Networks & Soft Computing, pp. 432-436.

3. Alwan I., Mohammed F. (2016), “Image Hiding Using Discrete Cosine Transform”, J. Of College Of Education For Women, №27, pp. 393-399.

4. Nagpal C., Goel R. (2013), “Modified quantization based steganography for color images”, International Journal of Electrical and Electronics Engineering, №2, pp. 9-17.

5. Akhmametieva A.V, Baraniuk A.A. (2019), “Modification of the steganographic method of embedding a digital watermark into image based on a wavelet transform”, Informatika ta matematichni metody v modelyvanny [Informatics and mathematical methods in modelling], №1, pp. 76-87.

6. Singh B. (2017), “Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR”, Journal of Emerging Research in Management &Technology, №8, pp. 230-234.

7. Jabbar K., Tuieb B. (2015), “Compare Between DCT and DWT for Digital Watermarking in Color Image”, Information and Knowledge Management, №5 (7), pp. 22-31.

8. Singh N. (2019), “High PSNR based Image Steganography”, International Journal of Advanced Engineering Research and Science, №1, pp. 109-115.

9. Al-Haj A. (2007), “Combined DWT-DCT Digital Image Watermarking”, Journal of Computer Science, №3 (9), pp. 740-746.

10. Akter A., Tajnina N. (2014), “Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm”, International Conference on Informatics, Electronics & Vision (ICIEV), №10, pp.1-6.
11. Benoraira A., Benmahammed K., Boucenna N. (2017), “Blind image watermarking technique based on differential embedding in DWT and DCT domains”, Benoraira et al. EURASIP Journal on Advances in Signal Processing, №55. – pp. 1-11.
12. Rahman M. (2013), “A dwt, dct and svd based watermarking technique to protect the image piracy”, International Journal of Managing Public Sector Information and Communication Technologies, №4 (2), pp. 1-12.
13. Melnyk M. (2014) “Method of estimation of steganographic algorithm stability to compression attacks”, Zbirnyk naukovykh prats’ Viys’kovoho instytutu Kyyivs’koho natsional’noho universytetu imeni Tarasa Shevchenka [Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv], № 44, pp. 121-128.

Ph.D. Akhmametieva A.V., Baraniuk A.A.

DEVELOPMENT OF A SYSTEM FOR DIGITAL WATERMARKS EMBEDDING INTO IMAGES BASED ON DCT-LWT-SVD

Copyright protection of digital content is a rather actual problem of humanity in the 21st century. Misuses of multimedia content is very common, and their number is growing with each passing day. One type of copyright protection is the embedding of digital watermark (DW) in the content.

In this paper a new method of embedding digital watermark into image using discrete cosine transform, lifting wavelet transform (LWT) with maternal wavelet "Dobeshi-8" and singular coefficients decomposition is proposed. Embedding is performed into the first singular number of the low frequency wavelet transform region. As a digital watermark, we will use a grayscale image normalized to a range from zero to ten to provide a high peak signal-to-noise ratio (PSNR).

The research analyzed the developed method: the method of embedding and detecting information was tested for its resistance to various types of attacks, namely: application of noise overlay (Gauss and pulse noise, "salt and pepper"), "unsharp" filter and median filter, and compression attack (with quality coefficients for a complete container from 60 to 100). As a result of the conducted testing, it was established that the method is quite resistant to all the attacks, except for the "unsharp" filtering (the resulting performance is not satisfactory).

The method showed good results in peak signal-to-noise ratio - the average PSNR value is 50.5 dB, as well as high rates of similarity between the embedded DW and the extracted one - from 77% to 97.6% while saving the full container in a lossless format, and up to 53, 05 dB and 91.96% while saving the image in a lossless format (JPEG).

Keywords: steganography, digital watermark, discrete cosine transform, lifting wavelet transform, singular value decomposition, digital image.