

МОДИФІКАЦІЯ СТЕГАНОГРАФІЧНОГО МЕТОДУ ВБУДОВИ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ В ЗОБРАЖЕННЯ НА ОСНОВІ ВЕЙВЛЕТ- ПЕРЕТВОРЕННЯ

Г.В. Ахмаметьєва, Г.А. Баранюк, А.І. Казаков

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: anna-odessitka@mail.ru

В роботі запропоновано модифікацію стеганографічного методу вбудови цифрового водяного знаку в область вейвлет-перетворення цифрового зображення. Запропонований метод здійснює вбудову водяного знаку в високочастотні деталізуючі коефіцієнти трирівневого вейвлет-перетворення з використанням вейвлету Добеші-43, що забезпечує високу якість отриманого стеганоповідомлення, яке зберігається в форматі з втратами, що обумовлено широким розповсюдженням таких зображень у зв'язку з їх малим розміром. До цифрового водяного знаку застосовується дискретне косинусне перетворення, завдяки чому підвищується ефективність виявлення наявності водяного знаку у стеганоповідомленні. В роботі проводиться аналіз ефективності детектування цифрового водяного знаку в залежності від порогових значень, які визначають вибір деталізуючих коефіцієнтів, використовуваних для вбудови, в результаті якого встановлено, що підвищення порогів без застосування до водяного знаку дискретного косинусного перетворення призводить до значного погіршення точності детектування. І навпаки, запропонований метод з пороговими значеннями $T_1=80$ і $T_2=90$ вибору деталізуючих коефіцієнтів у поєднанні з дискретним косинусним перетворенням матриці водяного знаку дозволив підвищити відсоток правильно детектованих стеганоповідомлень. Результати проведених обчислювальних експериментів показали стійкість вкладення водяного знаку до атак стиском (навіть при якості зображення $QF=5$), накладання шуму, підвищення різкості, зсуву, для яких точність детектування становить в середньому 97%. Також метод є стійким до масштабування за умови $QF>50$. В роботі проводиться порівняння стійкості оригінального методу вбудови цифрового водяного знаку і різних варіацій запропонованої модифікації стеганографічного методу до комплексних атак (стиску у поєднанні з іншими видами обробки цифрових зображень).

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

Вступ

Сучасний розвиток інформаційних технологій та їх широке розповсюдження в соціумі призводять до масштабної миттєвої комунікації між кореспондентами з різних країн світу, обміну документами та мультимедійним даними через електронну пошту, соціальні мережі, месенджери тощо. Такий документообіг значно ускладнює захист авторських прав на інтелектуальну власність, адже будь-хто може скористатися чужим контентом, модифікувати його, видати за власний. Одним із засобів захисту інтелектуальної власності є вбудова в інформаційний контент цифрового водяного знаку (ЦВЗ), за допомогою якого власник може довести своє право на той чи інший контент, з використанням стеганографії, яка приховує сам факт існування у будь-якому цифровому контейнері додаткової інформації. Одними з найбільш розповсюджених об'єктів такого захисту є цифрові зображення (ЦЗ).

Серед стеганографічних методів вбудови ЦВЗ в ЦЗ можна виділити роботи [1-3], які використовують область дискретного косинусного перетворення (ДКП). Однак ці методи, не зважаючи на стійкість до стиску, не забезпечують надійності цілісності

сприйняття стеганоповідомлень, отримані значення PSNR не перевищують 40 дБ. Більш якісні стеганоповідомлення можна отримати, вбудовуючи ЦВЗ в область вейвлет-перетворення за допомогою методів [4-5], проте в роботі [4] не проведено дослідження щодо стійкості запропонованого методу до атак, а в роботі [5] спостерігається невисока точність виявлення ЦВЗ.

Таким чином, підвищення стійкості стеганографічної системи ЦВЗ до атак при збереженні надійності сприйняття стеганоповідомлення є надзвичайно важливою і актуальною задачею.

Мета і задачі дослідження

Метою роботи є підвищення стійкості до атак та забезпечення надійного детектування цифрових водяних знаків з стеганоповідомлень, сформованих стеганографічним методом вбудовування ЦВЗ в область вейвлет-перетворення цифрового зображення.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- проаналізувати вплив параметрів стеганографічного методу вбудовування ЦВЗ в область вейвлет-перетворення на ефективність детектування ЦВЗ;
- з урахуванням проведеного аналізу модифікувати стеганографічний метод вбудови ЦВЗ;
- провести оцінку ефективності запропонованого стеганографічного методу і порівняння його з аналогами.

Основна частина

За основу розроблювальної стеганографічної системи ЦВЗ було взято метод Dugad, Ratakonda і Ahuja [5], який здійснює вбудову водяного знаку в область вейвлет-перетворення. Додаткова інформація, в ролі якої виступає ЦВЗ – зображення в градаціях сірого, вбудовується в деталізовані коефіцієнти трирівневого вейвлет-перетворення на основі вейвлету Добеші-8, значення яких перевищують поріг $T_1 = 40$ за допомогою формули [5]

$$V'_i = V_i + \alpha \cdot |V_i| \cdot x_i, \quad (1)$$

де V_i – значення i -го деталізованого коефіцієнту, який перевищує поріг T_1 , V'_i – значення модифікованого i -го деталізованого коефіцієнту стеганоповідомлення, x_i – значення яскравості ЦВЗ в діапазоні від $[0, 1]$, α – масштабуючий коефіцієнт, $\alpha = 0.2$.

Детектування наявності в стеганоповідомленні ЦВЗ відбувається за наявності в детекторі водяного знаку наступним чином:

- стеганоповідомлення розкладається на три рівні вейвлет-перетворення, в матриці деталізованих коефіцієнтів обираються такі коефіцієнти, для яких виконується умова $\hat{V}_i > T_2 > T_1$, де \hat{V}_i – стеганоповідомлення з (можливо) спотвореннями каналу зв'язку або навмисними модифікаціями злоумисника, $T_2 = 50$;
- з використанням існуючої в детекторі копії оригінального ЦВЗ обчислюється взаємна кореляція за формулою [5]

$$z = \frac{1}{M} \sum_i \hat{V}_i \cdot x_i, \quad (2)$$

де M – число елементів ЦВЗ;

• обчислене значення z порівнюється з порогом S , який визначається за формулою [5]

$$S = \frac{\alpha}{2M} \sum_i |\hat{V}_i|. \quad (3)$$

Якщо $z > S$, то детектор визначає наявність ЦВЗ.

Система ЦВЗ, запропонована Dugad, Ratakonda і Ahuja, дозволяє виявляти наявність ЦВЗ в умовах стиску, накладання шуму та деяких афінних перетворень, але, як показав проведений на основі 200 цифрових зображень обчислювальний експеримент, спостерігаються досить низькі значення PSNR: в середньому від 29.35 дБ до 45.78 дБ (для $QF \in [50, 100]$ з кроком 5) в залежності від якості стиску (чим нижче значення QF , тим нижче значення PSNR) та характеристик самого зображення (низька якість та чіткість контейнеру, його невеликий розмір, розмиті контури, тощо).

Одним з шляхів підвищення якості стеганоповідомлень, отриманих в результаті вбудови ЦВЗ, є збільшення порогових значень T_1, T_2 , інший – заміна вейвлет-фільтру. Був проведений обчислювальний експеримент, в результаті якого вдалося збільшити значення PSNR в середньому від 31.87 дБ до 47.15 дБ (для $QF \in [50, 100]$ з кроком 5) при використанні вейвлету Добеші-43. Подальша зміна вейвлету не призводила до значного покращення якості стеганоповідомлень. В результаті аналізу матриць деталізованих коефіцієнтів, отриманих трирівневим перетворенням Добеші-43, оптимальними з точки зору якості зображення та забезпечення необхідної пропускну здатності, значеннями порогів T_1 і T_2 прийнято $T_1 = 80, T_2 = 90$. Однак дослідження, спрямовані на оцінку ефективності детектування ЦВЗ, показали, що одночасна заміна вейвлет-фільтру та підвищення порогових значень T_1 і T_2 призводять до погіршення правильно виявлених стеганоповідомлень, захищених ЦВЗ.

Для забезпечення надійного детектування ЦВЗ в стеганоповідомленні була проведена інтеграція методу Dugad, Ratakonda і Ahuja з методом, запропонованим в [6] Mei Jiansheng, Li Sukang і Tan Xiaomei. На відміну від розглянутого вище методу Dugad, Ratakonda і Ahuja, який представляє собою стеганографічну систему ЦВЗ напівзакритого типу [7], запропонований в роботі [6] метод спрямований на вилучення ЦВЗ за наявності у детектора оригінального контейнеру, тобто система ЦВЗ закритого типу II [7]. Оскільки важливішою задачею для ЦВЗ є правильне детектування наявності вбудованого водяного знаку в стеганоповідомленні, що зазнало випадкових або навмисних спотворень, модифікуємо метод Mei Jiansheng, Li Sukang і Tan Xiaomei як систему ЦВЗ напівзакритого типу.

Згідно з методом [6] перед вбудовою ЦВЗ в контейнер обчислюється ДКП матриці водяного знаку, після чого відбувається його вбудова в контейнер за формулою

$$V'_i = V_i + \alpha \cdot x_i. \quad (4)$$

Таким чином, зазначимо основні кроки модифікованої стеганографічної системи ЦВЗ.

Вбудова ЦВЗ.

Для цифрового зображення в градаціях сірого I (колірної складової кольорового ЦЗ) розміром $m \times n$ і ЦВЗ в градаціях сірого Z розміром $h \times w$:

Крок 1. Побудувати трирівневе вейвлет-перетворення контейнеру I на основі вейвлет-фільтру W . В результаті отримуємо матрицю апроксимуючих коефіцієнтів A і три матриці деталізованих коефіцієнтів H, V, D розміром $m_3 \times n_3$.

Крок 2. Вибір матриці деталізованих коефіцієнтів для вбудови ЦВЗ. Матриця для вбудови ЦВЗ обирається таким чином, щоб кількість коефіцієнтів, більших T_1 , перевищувала $k = h \cdot w$. Далі обрану матрицю детальних коефіцієнтів позначаємо як C .

Крок 3. Побудувати ДКП для ЦВЗ Z . Результат – матриця коефіцієнтів ДКП розміром $h \times w$, представлена у виді вектору X розміром k .

Крок 4. Вбудова ЦВЗ.

Якщо $C_{i,j} > T_1, i = \overline{1, m_3}, j = \overline{1, n_3}$, то $C_{i,j}' = C_{i,j} + \alpha \cdot X_g, g = \overline{1, k}$.

Крок 5. Побудувати обернене трирівневе вейвлет-перетворення на основі вейвлет-фільтру W .

Крок 6. Зберегти стеганоповідомлення.

Детектування наявності ЦВЗ.

Для стеганоповідомлення в градаціях сірого I' (колірної складової кольорового ЦЗ) розміром $m \times n$ і ЦВЗ в градаціях сірого Z розміром $h \times w$:

Крок 1. Побудувати трирівневе вейвлет-перетворення стеганоповідомлення I' на основі вейвлет-фільтру W . В результаті отримуємо матрицю апроксимуючих коефіцієнтів A' і три матриці деталізованих коефіцієнтів H', V', D' розміром $m_3 \times n_3$. Для детектування ЦВЗ використовується одна з матриць $H', V', D' - C'$, яка має містити ЦВЗ Z .

Крок 2. Побудувати ДКП для ЦВЗ Z . Результат – матриця коефіцієнтів ДКП розміром $h \times w$, представлена у виді вектору X розміром k .

Крок 3. Якщо $C'_{i,j} > T_2 > T_1, i = \overline{1, m_3}, j = \overline{1, n_3}$, обчислити взаємну кореляцію

$$z = \frac{1}{k} \sum_{i,j,g} C'_{i,j} \cdot X_g,$$

де $g = \overline{1, k}$.

Крок 4. Обчислити поріг $S = \frac{\alpha}{2k} \sum_{i,j} |C'_{i,j}|$.

Крок 5. Детектування наявності ЦВЗ.

Якщо $z > S$, то стеганоповідомлення I' містить ЦВЗ, інакше стеганоповідомлення I' не містить ЦВЗ.

В запропонованому стеганографічному методі ЦВЗ стеганоповідомлення зберігаються в форматі з втратами, адже такі зображення найбільш поширені у зв'язку з їх малим розміром і забезпеченням високої якості самого ЦЗ.

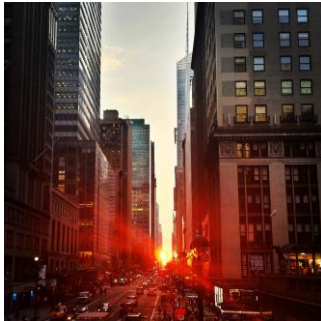
Приклад вбудови ЦВЗ в синю колірну складову ЦЗ запропонованим методом та методом [5] наведено на рисунку 1.

В наведеному прикладі стеганоповідомлення (рис.1, в, д) були збережені в форматі з втратами JPG з якістю $QF = 100$. При використанні методу [5] значення PSNR становить 52.036 дБ, а при використанні запропонованого методу – 53.0964 дБ.

Для оцінки ефективності запропонованого методу був проведений обчислювальний експеримент на основі 200 кольорових ЦЗ при використанні різних ЦВЗ, які були вбудовані в синю колірну складову контейнерів. В трирівневому вейвлет-перетворенні для вбудови ЦВЗ використовувалися вертикальні деталізовані коефіцієнти. Обчислювальні експерименти проводилися для чотирьох варіацій методів:

- метод Dugad, Ratakonda і Ahuja з використанням вейвлет-фільтру Добеші-8 та порогами $T_1 = 40, T_2 = 50 - M1$;

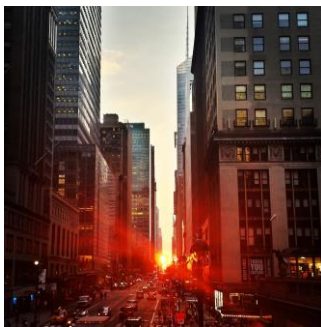
- метод Dugad, Ratakonda і Аһуја з використанням вейвлет-фільтру Добеші-43 та порогами $T_1 = 80, T_2 = 90$ – М2;
- запропонований метод з використанням вейвлет-фільтру Добеші-8 та порогами $T_1 = 40, T_2 = 50$ – М3;
- запропонований метод з використанням вейвлет-фільтру Добеші-43 та порогами $T_1 = 80, T_2 = 90$ – М4.



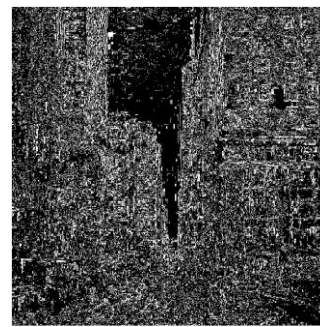
а



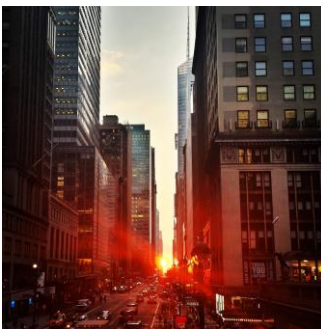
б



в



г



д



е

Рис. 1. Приклад вбудови ЦВЗ в цифрове зображення: а – оригінальний контейнер; б – ЦВЗ; в – стеганоповідомлення, отримане вбудовою ЦВЗ в контейнер методом Dugad, Ratakonda і Аһуја при використанні вейвлет-фільтру Добеші-8 і $T_1 = 40, T_2 = 50$; г – розміщення ЦВЗ в матриці синьої колірної складової стеганоповідомлення в); д – стеганоповідомлення, отримане вбудовою ЦВЗ в контейнер запропонованим методом при використанні вейвлет-фільтру Добеші-43 і $T_1 = 80, T_2 = 90$; е – розміщення ЦВЗ в матриці синьої колірної складової стеганоповідомлення д)

Ефективність методів будемо оцінювати як долю правильно виявлених ЦВЗ в стеганоповідомленні. Результати обчислювального експерименту для зазначених методів з атакою стиску при різних значеннях якості QF наведені в таблиці 1.

Таблиця 1.

Ефективність детектування наявності ЦВЗ в стеганоповідомленні за умови атаки стиском

<i>QF</i>	100	95	90	85	80	75	70	65	60	55
M1	0.765	0.75	0.76	0.75	0.75	0.74	0.74	0.73	0.73	0.73
M2	0.44	0.41	0.4	0.4	0.39	0.39	0.39	0.4	0.4	0.4
M3	0.915	0.91	0.94	0.89	0.9	0.91	0.93	0.9	0.94	0.96
M4	0.995	0.99	0.98	0.98	0.96	0.95	0.97	0.95	0.96	0.95
<i>QF</i>	50	45	40	35	30	25	20	15	10	5
M1	0.74	0.75	0.73	0.72	0.72	0.73	0.74	0.73	0.71	0.71
M2	0.39	0.4	0.38	0.39	0.38	0.39	0.38	0.39	0.39	0.4
M3	0.87	0.88	0.93	0.93	0.94	0.93	0.94	0.94	0.92	0.9
M4	0.97	0.98	0.96	0.98	0.97	0.98	0.98	0.98	0.975	0.98

Як видно з таблиці 1, найкращі результати детектування ЦВЗ в умовах стиску характерні для запропонованого методу (варіації M3 і M4), найгірший результат – для варіації методу Dugad, Ratakonda і Ahuja M2, тому в подальших експериментах він не буде розглядатися.

Окрім атаки стиском можуть використовуватися як будь-які навмисні атаки зловмисника, так і випадкові спотворення в процесі передачі стеганоповідомлення по каналу зв'язку. В таблицях 2 і 3 наведено порівняння ефективності детектування ЦВЗ в умовах атак для методів M1, M3 і M4 при різних значеннях параметру *QF*.

Таблиця 2.

Порівняння ефективності детектування наявності ЦВЗ в стеганоповідомленні за умови атак для методів M1, M3, M4 при $QF \in [55, 100]$

<i>QF</i>		100	95	90	85	80	75	70	65	60	55
Атака	Параметри	M1									
Гаусів шум	$m = 0.01,$ $d = 0.0005$	0.755	0.75	0.74	0.74	0.74	0.73	0.73	0.73	0.73	0.73
	$m = 0.01,$ $d = 0.00005$	0.765	0.76	0.76	0.74	0.75	0.74	0.73	0.74	0.74	0.74
	$m = 0.01,$ $d = 0.000005$	0.765	0.76	0.76	0.76	0.74	0.73	0.74	0.74	0.74	0.74
Пуасонівський шум		0.715	0.73	0.73	0.72	0.71	0.7	0.72	0.71	0.71	0.72
Мультиплікативний шум	$d = 0.001$	0.755	0.75	0.75	0.75	0.75	0.74	0.74	0.74	0.74	0.73
	$d = 0.0001$	0.765	0.75	0.76	0.75	0.75	0.74	0.73	0.74	0.73	0.74
	$d = 0.00001$	0.765	0.75	0.76	0.75	0.75	0.74	0.73	0.74	0.74	0.73
Імпульсний шум	$d = 0.001$	0.755	0.74	0.75	0.74	0.74	0.73	0.74	0.74	0.74	0.74
Фільтр підвищення різкості «unsharp»		0.77	0.77	0.76	0.77	0.76	0.75	0.76	0.76	0.76	0.76
Зсув	$sh_x = 0.15,$ $sh_y = 0.25$	0.79	0.76	0.77	0.76	0.76	0.76	0.75	0.75	0.75	0.75
Масштаб	$s_x = 1.15,$ $s_y = 0.85$	0.81	0.81	0.81	0.8	0.75	0.75	0.75	0.75	0.75	0.75

Продовження таблиці 2.

Поворот	30°	0.82	0.81	0.81	0.81	0.81	0.81	0.8	0.75	0.75	0.75
Атака	Параметри	М3									
Гаусів шум	$m = 0.01,$ $d = 0.0005$	0.915	0.92	0.93	0.91	0.91	0.87	0.94	0.88	0.97	0.95
	$m = 0.01,$ $d = 0.00005$	0.955	0.92	0.93	0.91	0.92	0.91	0.95	0.89	0.94	0.95
	$m = 0.01,$ $d = 0.000005$	0.91	0.93	0.97	0.93	0.91	0.95	0.96	0.91	0.95	0.92
Пуасонівський шум		0.865	0.89	0.92	0.94	0.96	0.89	0.93	0.94	0.93	0.91
Мультиплікативний шум	$d = 0.001$	0.915	0.91	0.9	0.94	0.93	0.9	0.92	0.94	0.95	0.92
	$d = 0.0001$	0.945	0.93	0.93	0.9	0.91	0.93	0.93	0.91	0.96	0.92
	$d = 0.00001$	0.925	0.91	0.94	0.93	0.9	0.92	0.96	0.94	0.96	0.91
Імпульсний шум	$d = 0.001$	0.925	0.95	0.95	0.91	0.93	0.91	0.95	0.92	0.96	0.93
Фільтр підвищення різкості «unsharp»		0.87	0.91	0.89	0.94	0.93	0.91	0.92	0.91	0.9	0.91
Зсув	$sh_x = 0.15,$ $sh_y = 0.25$	0.94	0.93	0.95	0.91	0.92	0.93	0.94	0.93	0.95	0.96
Масштаб	$s_x = 1.15,$ $s_y = 0.85$	0.51	0.65	0.45	0.41	0.49	0.69	0.69	0.37	0.38	0.34
Поворот	30°	0.5	0.5	0.45	0.45	0.45	0.6	0.65	0.36	0.4	0.6
Атака	Параметри	М4									
Гаусів шум	$m = 0.01,$ $d = 0.0005$	0.995	0.99	0.98	0.98	0.96	0.95	0.97	0.95	0.96	0.95
	$m = 0.01,$ $d = 0.00005$	0.985	0.99	0.99	0.98	0.98	0.99	0.94	0.95	0.95	0.98
	$m = 0.01,$ $d = 0.000005$	0.985	1	0.98	0.99	0.97	0.94	0.96	0.98	0.98	1
Пуасонівський шум		0.975	0.95	0.98	1.01	0.96	0.95	0.94	0.97	0.97	0.97
Мультиплікативний шум	$d = 0.001$	0.975	0.95	0.98	1.01	0.96	0.95	0.94	0.97	0.97	0.97
	$d = 0.0001$	0.985	0.99	1	0.99	0.99	0.96	0.97	0.99	0.97	0.95
	$d = 0.00001$	0.995	1	0.98	0.97	0.97	0.97	0.95	0.97	0.98	0.97
Імпульсний шум	$d = 0.001$	0.995	1	0.98	0.97	0.96	0.95	0.94	0.99	0.96	0.95
Фільтр підвищення різкості «unsharp»		0.895	0.95	0.92	0.95	0.94	0.97	0.97	0.97	0.97	0.97
Зсув	$sh_x = 0.15,$ $sh_y = 0.25$	0.895	0.95	0.92	0.95	0.94	0.97	0.97	0.97	0.97	0.97
Масштаб	$s_x = 1.15,$ $s_y = 0.85$	1	1	0.99	0.97	0.98	0.96	0.99	0.97	0.98	0.98
Поворот	30°	0.63	0.57	0.45	0.56	0.47	0.67	0.59	0.58	0.58	0.63

Таблиця 3.

Порівняння ефективності детектування наявності ЦВЗ в стеганоповідомленні за умови атак для методів М1, М3, М4 при $QF \in [5, 50]$

QF		50	45	40	35	30	25	20	15	10	5
Атака	Параметри	М1									
Гаусів шум	$m = 0.01,$ $d = 0.0005$	0.73	0.72	0.73	0.72	0.71	0.71	0.73	0.73	0.7	0.71
	$m = 0.01,$ $d = 0.00005$	0.73	0.74	0.74	0.72	0.71	0.73	0.74	0.73	0.71	0.71
	$m = 0.01,$ $d = 0.000005$	0.74	0.74	0.74	0.72	0.71	0.72	0.74	0.74	0.71	0.71
Пуасонівський шум		0.72	0.72	0.69	0.72	0.71	0.7	0.71	0.69	0.7	0.7
Мультиплікативний шум	$d = 0.001$	0.73	0.73	0.72	0.72	0.73	0.73	0.73	0.73	0.71	0.71
	$d = 0.0001$	0.74	0.75	0.74	0.71	0.72	0.74	0.74	0.74	0.71	0.71
	$d = 0.00001$	0.74	0.74	0.74	0.72	0.72	0.73	0.74	0.73	0.71	0.71
Імпульсний шум	$d = 0.001$	0.74	0.74	0.73	0.73	0.72	0.72	0.72	0.72	0.71	0.71
Фільтр підвищення різкості «unsharp»		0.75	0.75	0.74	0.74	0.74	0.74	0.74	0.74	0.74	0.74
Зсув	$sh_x = 0.15,$ $sh_y = 0.25$	0.75	0.76	0.74	0.74	0.75	0.74	0.75	0.73	0.71	0.71
Масштаб	$s_x = 1.15,$ $s_y = 0.85$	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.7	0.64
Поворот	30°	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.7	0.69
Атака	Параметри	М3									
Гаусів шум	$m = 0.01,$ $d = 0.0005$	0.9	0.93	0.9	0.89	0.93	0.93	0.94	0.88	0.9	0.9
	$m = 0.01,$ $d = 0.00005$	0.92	0.91	0.92	0.93	0.93	0.9	0.92	0.89	0.97	0.9
	$m = 0.01,$ $d = 0.000005$	0.92	0.9	0.94	0.89	0.95	0.95	0.94	0.94	0.93	0.9
Пуасонівський шум		0.92	0.96	0.94	0.92	0.95	0.9	0.88	0.93	0.89	0.9
Мультиплікативний шум	$d = 0.001$	0.93	0.9	0.94	0.97	0.95	0.91	0.95	0.92	0.92	0.9
	$d = 0.0001$	0.92	0.94	0.92	0.89	0.93	0.95	0.9	0.92	0.94	0.9
	$d = 0.00001$	0.87	0.94	0.92	0.91	0.95	0.95	0.9	0.91	0.94	0.9
Імпульсний шум	$d = 0.001$	0.91	0.92	0.9	0.92	0.95	0.93	0.94	0.89	0.89	0.9
Фільтр підвищення різкості «unsharp»		0.94	0.93	0.88	0.92	0.92	0.94	0.97	0.9	0.92	0.9
Зсув	$sh_x = 0.15,$ $sh_y = 0.25$	0.9	0.91	0.95	0.94	0.96	0.93	0.96	0.95	0.94	0.9
Масштаб	$s_x = 1.15,$ $s_y = 0.85$	0.37	0.37	0.69	0.69	0.37	0.41	0.37	0.41	0.39	0.5

Продовження таблиці 3.

Поворот	30°	0.64	0.4	0.65	0.37	0.44	0.4	0.36	0.37	0.34	0.4
Атака	Параметри	M4									
Гаусів шум	$m = 0.01,$ $d = 0.0005$	0.95	0.94	0.97	0.98	0.97	0.95	0.97	0.97	0.935	0.945
	$m = 0.01,$ $d = 0.00005$	0.95	0.98	1	0.99	0.95	0.95	0.98	0.94	0.955	0.945
	$m = 0.01,$ $d = 0.000005$	0.96	0.99	0.99	0.94	0.97	0.97	0.99	0.97	0.935	0.955
Пуасонівський шум		0.98	0.96	0.96	0.96	0.97	0.95	0.97	0.98	0.965	0.975
Мультиплі- кативний шум	$d = 0.001$	0.95	0.98	0.98	0.96	0.98	0.98	0.95	0.97	0.975	0.955
	$d = 0.0001$	0.98	0.98	0.99	0.97	0.98	0.95	0.98	0.98	0.965	0.955
	$d = 0.00001$	0.97	0.99	0.97	0.97	1	0.96	1	0.95	0.955	0.975
Імпульсний шум	$d = 0.001$	0.96	0.98	0.95	0.98	0.98	0.97	0.97	0.98	0.945	0.955
Фільтр підвищення різкості «unsharp»		0.96	0.93	0.93	0.96	0.96	0.93	0.94	0.96	0.965	0.985
Зсув	$sh_x = 0.15,$ $sh_y = 0.25$	1	0.99	0.98	0.98	1	0.98	0.98	0.99	0.98	0.99
Масштаб	$s_x = 1.15,$ $s_y = 0.85$	0.63	0.7	0.48	0.54	0.54	0.51	0.47	0.58	0.68	0.61
Поворот	30°	0.54	0.59	0.63	0.48	0.59	0.53	0.49	0.53	0.46	0.47

Порівнюючи варіації запропонованого методу вбудови ЦВЗ M3 і M4 можна зробити висновок, що використання вейвлет-фільтру Добеші-43 разом з порогоми $T_1 = 80, T_2 = 90$ дає кращі результати детектування наявності ЦВЗ в цифровому контенті при забезпеченні високої якості стеганоповідомлень.

Висновки

В роботі запропоновано модифікацію стеганографічного методу вбудови ЦВЗ в область вейвлет-перетворення ЦЗ. В ході дослідження впливу порогових значень T_1, T_2 і обраного вейвлет-фільтру було встановлено, що використання вейвлету Добеші-43 у порівнянні з Добеші-8 дає кращі показники цілісності сприйняття стеганоповідомлення (значення PSNR вище при використанні Добеші-43), однак одночасне збільшення порогових значень T_1, T_2 призводить до погіршення результатів детектування ЦВЗ.

З метою покращення виявлення наявності ЦВЗ в стеганоповідомленні до ЦВЗ перед вбудовою в контейнер було застосовано ДКП. Це дозволило забезпечити високу точність детектування ЦВЗ не тільки в умовах стиску, а й під впливом додаткових атак, таких як шум, підвищення різкості, деякі афінні перетворення, зберігаючи при цьому високу якість сформованого стеганоповідомлення.

Проведені обчислювальні експерименти, спрямовані на визначення ефективності запропонованого стеганографічного методу, показали, що метод є стійким до стиску,

накладання шуму, підвищення різкості та деяких афінних перетворень (зсуву та масштабування при $QF > 50$).

Список літератури

1. Podilchuk, I. Image-Adaptive Watermarking Using Visual Models / I. Podilchuk, W. Zeng. // IEEE Journal on selected areas in communications. – 1998. – №4. – Pp. 525-539.
2. Chiou-Ting, Hsu. Multiresolution Watermarking for Digital Images / Hsu. Chiou-Ting, Ja-Ling Wu // IEEE Transactions on circuits and systems—II: Analog and digital signal processing. – 1998. – №8. – Pp. 1097-1101.
3. Pal, A. A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity / A. Pal, K. Naik, R. Agarwal. // The International Arab Journal of Information Technology. – 2019. – №1. – С. 116-124.
4. Baby, D. A Novel DWT based Image Securing Method using Steganography / D. Baby, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela // International Conference on Information and Communication Technologies (ICICT 2014). – 2015. – С. 612-618.
5. Dugat, R. A new wavelet-based scheme for watermarking images / R. Dugat, K. Ratakonda, N. Ahuja // Proceedings of the IEEE International Conference Image Processing. – 1998. – Pp. 357-372.
6. Jiansheng, M. A Digital Watermarking Algorithm Based On DCT and DWT / M. Jiansheng, Li Sukang and Tan Xiaomei // Proceedings of the 2009 International Symposium on Web Information Systems and Applications. – 2009. – Pp. 104-107.
7. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2017. – 262 с.

МОДИФИКАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ВСТРАИВАНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ИЗОБРАЖЕНИЕ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

А.В. Ахмаметьева, А.А. Баранюк, А.И. Казаков

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: anna-odessitka@mail.ru

В работе предложена модификация стеганографического метода встраивания цифрового водяного знака в область вейвлет-преобразования цифрового изображения. Предложенный метод осуществляет встраивание водяного знака в высокочастотные детализирующие коэффициенты трехуровневого вейвлет-преобразования с использованием вейвлета Добеши-43, который обеспечивает высокое качество полученного стеганосообщения, сохраняемого в формате с потерями, что обусловлено широким распространением таких изображений в связи с их малым размером. К цифровому водяному знаку применяется Дискретное косинусное преобразование, благодаря чему повышается эффективность выявления наличия водяного знака в стеганосообщении. В работе проводится анализ эффективности детектирования цифрового водяного знака в зависимости от пороговых значений, определяющих выбор детализирующих коэффициентов, используемых для погружения, в результате которого установлено, что повышение порогов без применения к водяному знаку Дискретного косинусного преобразования приводит к значительному ухудшению точности детектирования. И наоборот, предложенный метод с пороговыми значениями $T_1=80$ и $T_2=90$ выбора детализирующих коэффициентов в соединении с Дискретным косинусным преобразованием матрицы водяного знака позволил повысить процент правильно выявленных стеганосообщений. Результаты проведенных экспериментов показали стойкость вложения цифрового водяного знака к атакам сжатия (даже при качестве изображения $QF=5$), наложению шума, повышению резкости, сдвига, для которых точность детектирования составляет в среднем 97%. Также метод является стойким к масштабированию при условии $QF>50$. В работе проводится сравнение стойкости оригинального метода встраивания цифрового водяного знака и разных вариаций предложенной модификации стеганографического метода к комплексным атакам (сжатию в соединении с другими видами обработки цифровых изображений).

Ключевые слова: стеганография, цифровой водяной знак, вейвлет-преобразование, Дискретное косинусное преобразование, цифровое изображение.

MODIFICATION OF THE STEGANOGRAPHIC METHOD OF EMBEDDING A DIGITAL WATERMARK INTO IMAGE BASED ON A WAVELET TRANSFORM

A.V. Akhmametiyeva, A.A. Baranuk, A.I. Kazakov

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: anna-odessitka@mail.ru

The paper proposes a modification of the steganographic method of embedding a digital watermark into Wavelet transform domain of a digital image. The proposed method embeds a watermark in the high-frequency detail coefficients of a three-level Wavelet transform using the Dobeshi-43 wavelet, which ensures the high quality of the resulting stego. Stego is a result of embedding of digital watermark into container and is saved in a losses format that is caused by wide dissemination of such images due to their small size. Discrete cosine transform is applied to a digital watermark, thereby increasing the efficiency of detecting the presence of a watermark in a stego. In work the analysis of efficiency of detecting of the digital watermark depending on the threshold values defining the choice of the detailing coefficients used for embedding is carried out. A result of this analysis is establishment the fact that increase in thresholds without application of Discrete cosine transformation to the watermark leads to considerable deterioration in accuracy of detecting. Conversely, the proposed method with the threshold values $T_1=80$ and $T_2=90$ of the choice of detailing coefficients in conjunction with the Discrete Cosine Transformation of the watermark matrix increased the percentage of correctly identified stegos. The results of the experiments showed the resistance of embedding a digital watermark to compression attacks (even with image quality $QF=5$), imposing noise, sharpening, shifting, for which the detection accuracy averages 97%. Also, the method is resistant to scaling provided $QF>50$. This paper compares the resistance of the original method of embedding a digital watermark and different variations of the proposed modification of the steganographic method to complex attacks (compression in combination with other types of digital image processing).

Keywords: steganography, digital watermark, Wavelet-transform, Discrete cosine transformation, digital image