DOI 10.15276/imms.v11.no1-2.27
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 1-2, pp. 27-35

РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДУ ВБУДОВИ БІНАРНОГО ЦИФРОВОГО ВОДЯНОГО ЗНАКУ В ЗОБРАЖЕННЯ НА ОСНОВІ ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ

Г.В. Ахмаметьєва, В.О. Кирилюк

Державний університет «Одеська політехніка»,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: a.v.akhmametieva@opu.ua

В даній роботі запропоновано стеганографічний метод вбудови бінарного цифрового водяного знаку (ЦВЗ) в середньочастотні коефіцієнти дискретного косинусного перетворення (ДКП) цифрового зображення. Для вбудовування ЦВЗ використовується один з середньочастотних коефіцієнтів двох колірних складових кольорового зображення: одна колірна складова застосовується для вбудови секретного коефіцієнту, який слугує віддзеркаленням змін в зображенні і сприяє підвищенню якості вилученого цифрового водяного знаку після накладення шумів на стеганоповідомлення. Друга колірна складова контейнеру використовується для вбудовування самого ЦВЗ. Запропонований метод передбачає автоматичний вибір колірних складових контейнера для вбудовування ЦВЗ та його попередню обробку для збільшення відстані між його елементами. Стаття містить основні кроки вбудовування і вилучення водяного знаку, а також результати обчислювальних експериментів, спрямованих на оцінку ефективності стеганографічного методу, та порівняння результатів з сучасними аналогами. Ефективність стеганографічного методу оцінюється показником візуальної якості стеганоповідомлень PSNR та різними показниками вилучення повідомлення. Стійкість до атак оцінюється показниками вилучення інформації з модифікованого стеганоповідомлення. В роботі проводиться аналіз розробленого методу при вбудові ЦВЗ в коефіцієнт (5,5) дискретного косинусного перетворення кожного блоку 8×8 цифрового зображення та деякого секретного коефіцієнта, що дорівнює 20. Результати проведених обчислювальних експериментів показали високу візуальну якість отриманих стеганоповідомлень (PSNR становить 50-58 дБ) та стійкість даного методу до шумів, а саме: мультиплікативного, пуасонівського, гаусового та «сіль і перець». У випадку з пуасонівським шумом, цифровий водяний знак видобувається майже без втрат, показники якості вилучення ЦВЗ не були нижчі за 0.97.

Ключові слова: стеганографія, бінарний цифровий водяний знак, дискретне косинусне перетворення, кольорове цифрове зображення

Вступ

В сучасному інформаційно-комунікаційному оточенні, яке охоплює всі сфери людського життя, з проникненням глобальної мережі Інтернет та, як наслідок, різноманітних засобів миттєвого зв'язку зростає необхідність захисту конфіденційних даних, що стосуються людини, організації, держави, та їх інтелектуальної власності, адже за останні роки набули значного поширення інциденти фальсифікації авторства на мультимедійні контенти, такі як аудіо, зображення і відео. Для вирішення проблеми захисту авторських прав в контент, який повинен бути захищений, вбудовують цифрові водяні знаки (ЦВЗ). Основною вимогою до систем вбудови ЦВЗ є стійкість стеганоповідомлень до атак, оскільки часто зловмисники намагаються або видалити наявний ЦВЗ, або підмінити власним, або унеможливити його коректне вилучення.

Серед наукових публікацій за останні роки, присвячених розробці стеганографічних методів, можна помітити тенденцію поєднання різних частотних перетворень, зокрема дискретного косинусного перетворення (ДКП), різновидів вейвлет-перетворення, сингулярного розкладу, тощо – це так звані «гібрідні» методи.

У статті [1] наведений метод вбудовування ЦВЗ, стійкий до кількох видів атаки. Запропонована схема водяних знаків базується на ліфтінговому вейвлет-перетворенні

(LWT) та розкладанні особливих значень (SVD). Запропонована робота зосереджена на підвищенні стійкості водяних знаків до атак, працюючи в частотній області, і тим самим покращуючи непомітність водяного знаку. За результатами експериментів, наведених в статті, для стеганоповідомлень забезпечується досить висока стійкість до шумів, однак якість стеганоповідомлень залишається невисокою, про що свідчать значення PSNR від 39 до 42 дБ.

У статті [2] алгоритм вбудовування ЦВЗ в контейнер складається з послідовних етапів дискретного вейвлет-перетворення, Z-перетворення, бідіагонального сингулярного розкладання (BSVD) та перетворення Арнольда. Виходячи з результатів, що представленні в статті, можна зробити висновок, що даний алгоритм показав досить високі показники PSNR для стандартних зображень, а саме 68,8925-72,6763 дБ, а при здійсненні різних атак, коефіцієнти кореляції були на високому рівні від 0,97 до 0,99.

В роботі [3] представлений спосіб вбудовування подвійного ЦВЗ з метою, щоб у разі виявлення першого водяного знаку зловмисником та подальшого його видалення, можна було за допомогою другого підтвердити авторські права та, як наслідок, звести старання зловмисника нанівець. Запропонований метод заснований на поєднання гомоморфічного перетворення, дискретного вейвлет-перетворення, SVD та перетворення Арнольда і забезпечує високу якість стеганоповідомлень (PSNR 59.1692-60.2320 дБ) та високу стійкість до атак (показники вилучення ЦВЗ наближені до 1).

Як правило, «гібридні» стеганографічні методи забезпечують високу якість стеганоповідомлень і стійкість до атак [4], але основним їх недоліком є висока обчислювальна складність, що обумовлено використанням декількох видів частотних перетворень. Ті ж методи, які застосовують лише один вид частотного перетворення, здебільшого не дають високої якості стеганоповідомлень при забезпеченні стійкості до деяких видів атак.

Зокрема, в статті [5] запропоновано вбудовувати два однакові ЦВЗ в коефіцієнти ДКП. За результатами експериментів, наведених в статті, можна зробити висновок, що даний метод є досить стійким до атак (показники вилучення інформації після атаки Гаусовим шумом становлять 0.9693-1), PSNR стеганоповідомлень становить 45.6513-47.6637 дБ, що для зображень в градаціях сірого є гарним результатом.

Ті методи, які засновані лише на використанні ДКП для кольорових зображень, [6, 7] забезпечують досить низьку якість стеганоповідомлень, виключенням є робота [8], в якій значення PSNR досягають 55 дБ.

Мета і задачі дослідження

Метою роботи є підвищення якості стеганоповідомлень шляхом розробки нового методу вбудови ЦВЗ в область ДКП цифрового зображення.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. розробити метод вбудови ЦВЗ на основі дискретного косинусного перетворення;
2. проаналізувати результати якості стеганоповідомлень і видобутку ЦВЗ для запропонованого стеганографічного методу;
3. провести оцінку ефективності розробленого методу і порівняння його з аналогами.

Основна частина

В статті пропонується блочний метод вбудови бінарного ЦВЗ в область дискретного косинусного перетворення кольорових цифрових зображень. Вбудовування біту ЦВЗ відбувається в середньочастотний коефіцієнт ДКП блоку 8×8 зображення шляхом заміни обраного коефіцієнту $d_{a,b}$ значенням $dw_{i,j}\cdot k$, де $dw_{i,j}$ - біт ЦВЗ, k - коефіцієнт, обчислений для певного зображення. Особливістю даного методу

є подвійне вбудовування ЦВЗ в контейнер, що дозволяє підвищити якість вилученого ЦВЗ. Це обумовлено тим, що переведення модифікованих коефіцієнтів ДКП блоку в просторову область впливає на якість вилучення ЦВЗ в тому сенсі, що приховані значення дещо змінені (спотворені), але наближені до дійсних. Повторне вбудовування ЦВЗ у вже модифікований контейнер дозволяє отримати вбудований ЦВЗ майже без помилок, і підвищити стійкість стеганоповідомлення до атак зашумленням, що підтверджують результати обчислювальних експериментів.

Основні кроки запропонованого методу наведені нижче.

Вбудовування ЦВЗ.

Для цифрового зображення в C розміром $m \times n \times 3$ і бінарного ЦВЗ dw розміром $h \times w$, при $m > 8h, n > 8w$ виконати наступне.

Крок 1. Попередня обробка ЦВЗ.

Модифікувати ЦВЗ за формулою:

$$dw_{i,j}{}' = dw_{i,j} \cdot 8 + 1,$$

де $dw_{i,j}$ і $dw_{i,j}{}'$ - значення (i, j)-го пікселя оригінального і модифікованого ЦВЗ відповідно.

Крок 2. Визначення колірних складових контейнера для вбудовування ЦВЗ.

2.1. Для блоків розміром 8×8 колірної складової I, $I \in \{R, G, B\}$ обчислити ДКП.

2.2. Знайти середнє значення всіх коефіцієнтів (a,b) ДКП блоків колірної складової I. Результат av^R, av^G, av^B.

2.3. Обрати для вбудови ЦВЗ колірну складову $I^{\max}$ з максимальним значенням серед av^R, av^G, av^B.

2.4. Обрати для вбудови значення $20 \cdot k$ матрицю I^{middle} з середнім по порядку значенням серед av^R, av^G, av^B. Оскільки коефіцієнт k є постійним для обраного зображення, має сенс вбудувати його лише в декілька блоків зображення, вибір яких може бути довільним.

Крок 3. Обчислити значення коефіцієнту k:

$$k = \begin{cases} \dfrac{mean\left(av^{I^{\max}}\right)}{mean(dw')}, & якщо\ mean\left(av^{I^{\max}}\right) \geq mean\left(av^{I^{middle}}\right) + 2, \\ \dfrac{mean\left(av^{I^{middle}}\right) + 2}{mean(dw')}, & якщо\ mean\left(av^{I^{\max}}\right) < mean\left(av^{I^{middle}}\right) + 2, \\ 1, & якщо\ mean\left(av^{I^{\max}}\right) < mean(dw'), \end{cases}$$

де $mean(dw')$ - середнє значення модифікованого ЦВЗ.

Крок 4. Вбудовувати значення $20 \cdot k$ в коефіцієнти ДКП (a,b) декількох блоків колірної складової I^{middle} за формулою:

$$d_{a,b}^{middle} = 20k,$$

де $d_{a,b}^{middle}$ - (a,b)-ий коефіцієнт ДКП блоку колірної складової I^{middle}.

Крок 5. Обчислити зворотне ДКП обраних блоків колірної складової I^{middle}. Округлити отримані значення яскравості блоків до цілих чисел в діапазоні від 0 до 255.

Крок 6. Вбудовування ЦВЗ.

Для блоків розміром 8×8 колірної складової $I^{\max}$:

5.1. Обчислити ДКП, результат $d^{\max}$.

5.2. Вбудовувати (i, j)-ий біт ЦВЗ в коефіцієнт (a,b) ДКП блоку за формулою:

$$d_{a,b}^{\max\prime} = \begin{cases} -dw_{i,j}{}' \cdot k, & якщо\ d_{a,b}^{\max} < 0, \\ dw_{i,j}{}' \cdot k, & якщо\ d_{a,b}^{\max} \geq 0, \end{cases}$$

де $d_{a,b}^{\max}$ - (a,b)-ий коефіцієнт ДКП блоку зображення.

5.3. Обчислити зворотне ДКП блоку колірної складової $I^{\max}$. Округлити отримані значення яскравості блоків до цілих чисел в діапазоні від 0 до 255.

Крок 7. Сформувати нове стеганоповідомлення S.

Крок 8. Повторити кроки 4-7 для зображення S, використовуючи коефіцієнт k, обчислений в кроці 3, та обрані в кроці 2 колірні складові $I^{\max}$ і I^{middle}.

Видобування ЦВЗ.

Для цифрового зображення в S розміром $m\times n\times 3$ виконати наступне.

Крок 1. Визначення колірних складових контейнера для вилучення ЦВЗ.

1.1. Для блоків розміром 8×8 колірної складової I, $I \in \{R,G,B\}$ обчислити ДКП.

1.2. Знайти середнє значення всіх коефіцієнтів (a,b) ДКП блоків колірної складової I. Результат av^R, av^G, av^B.

1.3. Обрати для вилучення ЦВЗ колірну складову $I^{\max}$ з максимальним значенням серед av^R, av^G, av^B.

1.4. Обрати для вилучення значення k матрицю I^{middle} з середнім по порядку значенням серед av^R, av^G, av^B.

Крок 2. Видобування значення k з коефіцієнтів ДКП (a,b) декількох блоків колірної складової I^{middle} з подальшим знаходженням їх середнього арифметичного.

Крок 3. Вилучення ЦВЗ.

Для блоків розміром 8×8 колірної складової $I^{\max}$:

3.1. Обчислити ДКП, результат $d^{\max}$.

3.2. Вилучити біт ЦВЗ з коефіцієнту (a,b) ДКП блоку за формулою

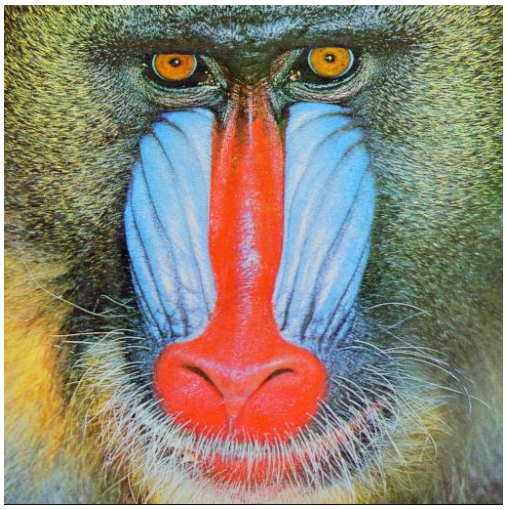
$$dw'_{ij} = \left| \frac{d_{a,b}{}' \cdot 20}{k} \right|.$$

3.3. Отримане значення відкоригувати у відповідності до формули:

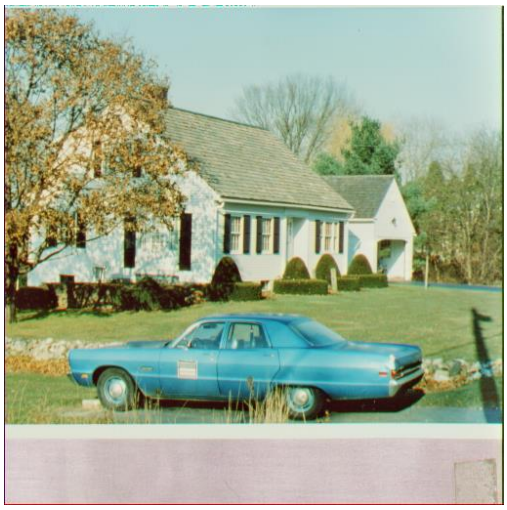
$$dw_{i,j}'' = \begin{cases} 1, & якщо\ dw_{i,j}' > 4.5, \\ 0, & якщо\ dw_{i,j}' \le 4.5, \\ 0, & якщо\ dw_{i,j}' = NaN. \end{cases}$$

Крок 4. Сформувати вихідний ЦВЗ.

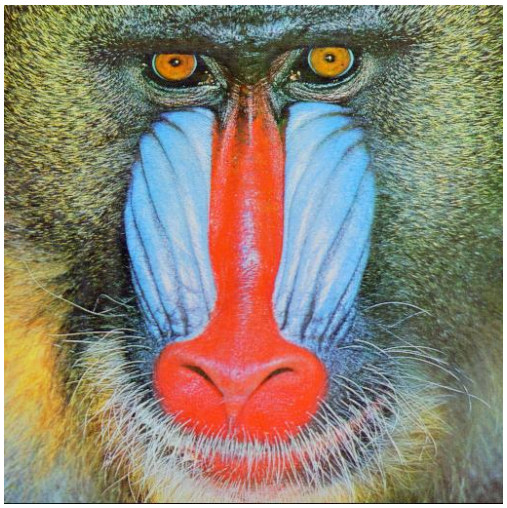
Для оцінки ефективності запропонованого методу був проведений обчислювальний експеримент на основі 200 цифрових зображень, та кількох ЦВЗ. Приклад вбудови та вилучення ЦВЗ в стандартні зображення показаний на рис.1.



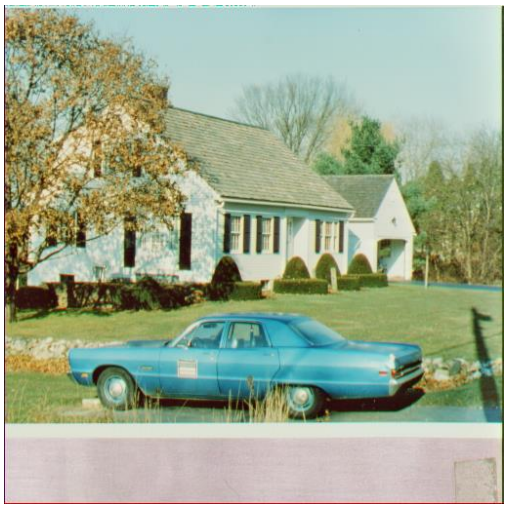
а



б



в



г

д

е

Рис.1. Приклад вбудови ЦВЗ в зображення: а, б – оригінальні контейнери; в, г – стеганоповідомлення, отримані вбудовою ЦВЗ в контейнери; д, е – вилучені ЦВЗ з стеганоповідомлень в і г відповідно

Якість отриманих стеганоповідомлень будемо оцінювати показниками MSE і PSNR, якість вилучення ЦВЗ з стеганоповідомлення показниками P [9], NCC [10], NC [11], BCR [12], SIM [13], що обумовлено використанням різними авторами різних показників, які обчислюються за формулами:

$$P = \frac{\textit{Кількість біт ЦВЗ, вилучених вірно}}{L},$$

$$NCC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{L},$$

де p_i - біти вбудованого ЦВЗ, $\overline{p_i}$ - біти вилученого ЦВЗ, $p_i, \overline{p_i} \in \{0,1\}, i = \overline{1,L}$; $p_i' = 1$, якщо $p_i = 1$, і $p_i' = -1$, якщо $p_i = 0$; $\overline{p_i}' = 1$, якщо $\overline{p_i} = 1$, і $\overline{p_i}' = -1$, якщо $\overline{p_i} = 0$, тобто $p_i' \times \overline{p_i}' \in \{-1,1\}$.

$$NC = \frac{\sum_{l=0}^{L-1} dw_l \cdot dw_l'}{\sum_{l=0}^{L-1} dw_l^{\,2}}, \qquad SIM = \frac{\sum_{l=0}^{L-1} dw_l \cdot dw_l'}{\sqrt{\sum_{l=0}^{L-1} dw_l^{\,2}} \cdot \sqrt{\sum_{l=0}^{L-1} dw_l'^{2}}}, \qquad BCR = \frac{1}{L}\sum_{l=0}^{L-1} \overline{dw_l \oplus dw_l'},$$

де dw_l - l-ий біт вбудованого ЦВЗ довжиною L, dw_l' - l-ий біт вилученого ЦВЗ, $\oplus$ - операція XOR.

Результати експериментів для зображень в умовах відсутності атак та атак накладання шумів продемонстровані в таблиці 1, де остання колонка «СЗ ПВІ» означає середнє значення показників вилучення інформації, тобто середнє значення показників P, NCC, NC, BCR, SIM.

Таблиця 1

Ефективність методу вбудови ЦВЗ в кольорові зображення

	PSNR, дБ	NCC	BCR	SIM	NC	P	СЗ ПВІ
Оригінальні стеганоповідомлення	52.285	0.998	0.999	0.995	0.999	0.999	0.9983
Гаусів шум, $m = 0, d = 0.0001$	39.437	0.988	0.994	0.961	0.969	0.994	0.9811
Гаусів шум, $m = 0, d = 0.0005$	41.856	0.977	0.988	0.925	0.938	0.988	0.9632
Гаусів шум, $m = 0, d = 0.001$	29.741	0.918	0.959	0.742	0.780	0.959	0.8718
Пуасонівський шум	52.296	0.998	0.999	0.995	0.999	0.999	0.9983
«Сіль & перець», $d = 0.001$	34.590	0.982	0.991	0.949	0.986	0.991	0.9797
«Сіль & перець», $d = 0.005$	27.662	0.965	0.982	0.890	0.938	0.982	0.9515
«Сіль & перець», $d = 0.01$	24.712	0.943	0.971	0.827	0.897	0.971	0.9219
Мультиплікативний шум, $d = 0.0001$	43.669	0.998	0.999	0.994	0.998	0.999	0.9975
Мультиплікативний шум,	37.357	0.968	0.984	0.908	0.954	0.984	0.9595

$d = 0.0005$							
Мультиплікативний шум, $d = 0.001$	34.455	0.949	0.974	0.850	0.909	0.974	0.9313

З таблиці 1 видно, що для запропонованого методу характерна досить висока стійкість до атак накладання шумів, зокрема метод є майже нечутливим до накладання Пуасонівського шуму – всі показники вилучення ЦВЗ наближені до 1. Для Гаусового, мультиплікативного, «сіль & перець» шумів якість вилучення залежить від дисперсії шуму (чим менше дисперсія – тим менше помилок вилучення ЦВЗ), однак навіть для дисперсії 0.001 забезпечуються достатньо надійне вилучення ЦВЗ – середні значення показників вилучення інформації перевищують 0.92 за виключенням Гаусового шуму, однак і в цьому випадку середнє значення наближене до 0.9.

Для порівняння якості стеганоповідомлень для запропонованого методу та сучасних аналогів будемо використовувати показник PSNR. Однак слід зазначити, що в статтях різних авторів використовуються різні формули для обчислення MSE або PSNR, що позначається на результатах. Саме тому для коректного порівняння з аналогами будемо обчислювати показники MSE та PSNR за тими формулами, що наводяться в статтях. Якщо в статті формула не наведена, будемо вважати, що використовується стандартне обчислення цих показників:

$$MSE = \frac{1}{XY}\sum\left(C_{x,y} - S_{x,y}\right)^2, \;\; PSNR = 10 \cdot \lg\left(\left(\max C_{x,y}\right)^2 \Big/ MSE\right). \qquad (1)$$

Інші нестандартні, але розповсюджені формули обчислення MSE і PSNR наступні:

$$MSE = \frac{1}{XY}\sum\left(C_{x,y} - S_{x,y}\right)^2, \;\; PSNR = 10 \cdot \lg\left(256^2 \Big/ MSE\right); \qquad (2)$$

$$MSE = \frac{1}{\left(XY\right)^2}\sum\left(C_{x,y} - S_{x,y}\right)^2, \;\; PSNR = 10 \cdot \lg\left(255^2 \Big/ MSE\right). \qquad (3)$$

В таблиці 2 наведені показники PSNR, обчислені на основі формул (1)-(3) для стандартних зображень. Оскільки в літературних джерелах, взятих для порівняння, обчислювальні експерименти застосовують не всі розглянуті зображення, а й інші, в таблиці 3 наводиться порівняння середніх значень PSNR для результатів експериментів запропонованого методу і сучасних аналогів.

Таблиця 2

Порівняння показників PSNR запропонованого методу і сучасних аналогів для стандартних зображень

Зображення	PSNR (1), дБ		PSNR (2), дБ		PSNR (3), дБ	
	[6], 2018	Запропон. метод	[8], 2019	Запропон. метод	[7], 2016	Запропон. метод
Airplane	-	54.2871	55.56	59.0923	-	108.4825
Baboon	-	45.3975	51.22	50.2027	-	99.5829
House	-	53.7728	-	58.5810	-	107.9612
Lena	41.36	53.3097	-	58.1149	32.15	107.4951
Peppers	-	54.24	-	59.0452	-	108.4254
Pot	-	54.8241	-	59.6293	-	109.0095
Sailboat	-	51.4517	-	56.2569	-	105.6371

Таблиця 3

Порівняння середніх значень PSNR експериментів сучасних аналогів і запропонованого методу

	PSNR (1), дБ		PSNR (2), дБ		PSNR (3), дБ
[1], 2018	41.29	[2], 2019	55.1635	[3], 2016	34.7833
Запропонований метод	52.469	Запропонований метод	57.2746	Запропонований метод	106.6562

Як видно з таблиць 2 і 3, показники PSNR, отримані для запропонованого методу, набагато перевищують показники візуальної якості сучасних аналогів.

Висновки

В роботі розроблений стеганографічний метод вбудови бінарного ЦВЗ в область дискретного косинусного перетворення цифрового зображення. З метою покращення видобутку ЦВЗ при його вбудові, запропоновано комплекс операцій, завдяки яким вдається показати хороші результати при вилученні ЦВЗ, та зберегти досить високу візуальну якість стеганоповідомлень.

В ході проведення обчислювальних експериментів, спрямованих на оцінку ефективності запропонованого методу, було виявлено його високу стійкість до атак накладання шумів, зокрема до Пуасонівського шуму – вилучення ЦВЗ відбувається майже без помилок. Досить надійне вилучення інформації відбувається і при накладанні Гаусового, мультиплікативного, «сіль & перець» шумів з дисперсією 0.001 – показники вилучення в середньому наближені до 0.9, що також є гарним результатом.

Список літератури

1. Manasha Saqib, Sameena Naaz. An Improvement in Digital Image Watermarking Scheme Based on Singular Value Decomposition and Wavelet Transform. *Asian Journal of Computer Science and Technology*. 2019. Vol. 8, No. 1. P. 62-68.
2. Jayashree N., Bhuvaneswaran R.S. A Robust Image Watermarking Scheme Using Z-Transform, Discrete Wavelet Transform and Bidiagonal Singular Value Decomposition. *CMC-Tech Science Press.* 2019. Volume 58, No.1. P.263-285.
3. Priyank Khare, Vinay Kumar Srivastava. A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT. *Journal of Intelligent Systems.* 2021. Vol. 30, No. 1. P. 297-311.
4. Mahbuba Begum, Mohammad Shorif Uddin. Analysis of Digital Image Watermarking Techniques through Hybrid Methods, *Advances in Multimedia*. 2020. Volume 2020. P. 1-12.
5. Sunesh, R.Rama Kishore. A Novel and Efficient Blind Image Watermarking in Transform Domain. *Procedia Computer Science*. 2020. No.167. P. 1505-1514.
6. Rand A. Watheq, Fadi Almasalha, Mahmoud H. Qutqut. A New Steganography Technique using JPEG Images. *International Journal of Advanced Computer Science and Applications*. 2018. Vol. 9, No. 11. P.751-760.
7. Iman M.G. Alwan, Farah Jasim Mohammed. Image Hiding Using Discrete Cosine Transform. *J. Of College Of Education For Women*. 2016. Vol. 27 (1). P.393-399.
8. Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf,Hanafy M. Ali. Hiding data in images using steganography techniques with compression algorithms. *TELKOMNIKA*. 2019. Vol.17, No.3. P.1168-1175.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев: «МК-Пресс», 2006. 288 с.
10. Мельник, М.А. Методика оценки устойчивости стеганоалгоритма к сжатию. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2013. Вип. 44. С. 121-128.

11. Melad J. Saeed. A new technique based on chaotic steganography and encryption text in DCT domain for color image. *Journal of Engineering Science and Technology*. 2013. Vol. 8, No. 5. P. 508-520.
12. Benoraira A., Benmahammed K., Boucenna N. Blind image watermarking technique based on differential embedding in DWT and DCT domains. *EURASIP Journal on Advances in Signal Processing*. 2017. No.55. P. 1-11.
13. Jabbar K., Tuieb B. Compare Between DCT and DWT for Digital Watermarking in Color Image. *Information and Knowledge Management*. 2015. No.5 (7). P. 22-31.

DEVELOPMENT OF STEGANOGRAPHICAL METHOD OF BINARY DIGITAL WATER MARK INSERT INTO IMAGE BASED ON DISCRETE COSINUS TRANSFORMATION

A.V. Akhmametieva, V.O. Kyryliuk

State University «Odessa Polytechnic»

This paper describes a steganographic method of embedding a binary digital watermark into the mid-frequency coefficients of discrete cosine transform of a digital image. One of the mid-frequency coefficients of the two color components of a color image is used to embed the digital watermark: one color component is used to embed a secret coefficient which reflects changes in the image and helps to improve the quality of the extracted digital watermark after applying noise to the stego. The second color component of the container is used for embedding of the digital watermark. The proposed method involves the automatic selection of color components of the container for embedding the digital watermark and its pre-processing to increase the distance between its elements. The article contains the main steps of embedding and extracting of a digital watermark, as well as the results of computational experiments aimed at evaluating the efficiency of the steganographic method, and comparing the results with modern analogues. The efficiency of the steganographic method is evaluated by the indicator of visual quality PSNR of stego and various indicators of message extraction. Resistance to attacks is evaluated by indicators of extraction of information from the modified stego. The paper analyzes the developed method when embedding some secret coefficient equal to 20 and the digital watermark into the coefficient (5.5) of the discrete cosine transform of each 8×8 block of digital image is carried out. The results of computational experiments showed the high visual quality of the received stegan messages (PSNR is 50-58 dB) and the resistance of this method to noise, namely: multiplicative, Poisson, Gaussian and "salt and pepper". In the case of Poisson noise, the digital watermark is extracted almost without loss, the quality of extraction of the digital watermark was not lower than 0.97.

Keywords: steganography, binary digital watermark, Discrete cosine transformation, color digital image