УДК 004.056.5

к.т.н. **Ахмаметьєва Г.В.** (ОНПУ)
Безсонова М.Д. (ОНПУ)

DOI: https://doi.org/10.17721/2519-481X/2020/69-07

РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДУ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ НА ОСНОВІ ПЕРЕТВОРЕННЯ ФУР'Є

У сучасному інтернет-просторі в умовах постійного обміну інформацією зростає необхідність її захисту від несанкціонованого використання сторонніми особами, що можна забезпечити використанням стеганографічних методів, які дозволяють організувати канал прихованої комунікації.

У статті розроблений новий стеганографічний метод для цифрових зображень на основі швидкого перетворення Фур'є. В якості додаткової інформації можна використовувати як текстові повідомлення, так і зображення, переведені в бінарну послідовність. Для вбудови додаткової інформації використовуються блоки 2×2, для яких обчислюється швидке перетворення Фур'є. Вбудова повідомлення здійснюється шляхом модифікації абсолютної різниці між двома коефіцієнтами перетворення Фур'є блока. В кожний блок можна вбудувати до чотирьох біт бінарної послідовності.

Результати обчислювальних експериментів, спрямованих на оцінку ефективності запропонованого методу, показали, що забезпечується висока якість стеганоповідомлень (середні значення PSNR становлять 58-60 дБ) в порівнянні з сучасними аналогами при забезпеченні високої пропускної спроможності прихованого каналу зв'язку (0.75 та 1 біт/піксель). Середні значення показника точності вилучення додаткової інформації NCC становлять від 0.87 до 0,97 в залежності від обраної колірної складової і кількості біт, що вбудовуються. Точність вилучення повідомлення залежить від характеристик самого контейнеру – при наявності великої кількості блоків зі значеннями яскравості, близьких до 0 або 255 виникають помилки детектування. Однак дану проблему можна усунути попереднім аналізом контейнера.

Розроблений метод показав високу стійкість до атаки шумом «Сіль та перець» (d=0.01) при помітних спотвореннях заповненого контейнеру, а також до накладання Гаусового і мультиплікативного шумів за умови непомітних спотворень стеганоповідомлення.

Ключові слова: стеганографія, швидке перетворення Фур'є, цифрове зображення.

Вступ та аналіз останніх досліджень. Сучасний розвиток інформаційних технологій сприяє їх широкому поширенню серед населення. В наш час вже неможливо уявити передачу будь-якої інформації без використання мережі Інтернет, обмін інформацією є настільки масштабним процесом, що вже неможливо повністю контролювати весь ланцюжок проходження інформаційним контентом проміжних серверів, які і забезпечують миттєву доставку повідомлень від відправника до отримувача. Ніхто з законних власників інформації не може гарантувати неможливість її несанкціонованого використання сторонніми особами, що потребує додаткового захисту конфіденційної інформації. Оскільки в ряді країн обмежено використання криптографічних засобів, широке поширення отримали розробки в області стеганографії – застосування стеганографічних методів і програм дозволяє зберегти в таємниці сам факт наявності повідомлення (додаткової інформації) в будь-якому інформаційному контенті. В якості контейнера можуть виступати будь-які цифрові дані: текстові документи, зображення, аудіо, відео та інші. Результат вбудови повідомлення в контейнер будемо називати заповненим контейнером або стеганоповідомленням.

При розробці стеганографічних методів увага приділяється наступним важливим умовам:

– забезпечення високої цілісності сприйняття сформованого стеганоповідомлення у порівнянні з оригінальним, відсутністю помітних спотворень, які указували б на наявність додаткової інформації;

– забезпечення надійності вилучення повідомлення з заповненого контейнеру, що є неодмінним компонентом при організації каналу прихованої передачі інформації;

– по можливості забезпечувати високу пропускну спроможність прихованого каналу інформації, оскільки в більшості методів підвищення ємності контейнера призводить до погіршення якості стеганоповідомлення;

– в деякої мірі стеганографічні методи повинні забезпечувати стійкість до навмисних або ненавмисних атак.

Більшість останніх публікацій присвячені розробці стеганографічних методів, заснованих на дискретному косинусному перетворенні [1,2], вейвлет-перетворенні [3,4] або комбінації частотних перетворень [5,6], що хоч і призводить до стійкості до атак, але для даних методів характерно зменшення пропускної спроможності і складність реалізації, крім того не забезпечується висока якість стеганоповідомлення, про що свідчать невисокі значення PSNR. Однак методів, в основу яких покладено перетворення Фур'є, не так багато.

В роботі [7] запропонований стеганографічний метод забезпечує достатньо високу пропускну спроможність, однак значно залежить від обраних параметрів вбудови – висока якість стеганоповідомлень забезпечується лише при малих значеннях α, при значеннях $\alpha > 0.0001$ заповнений контейнер містить помітні спотворення. В роботах [8,9] отримані невисокі значення PSNR (37,6 і 32,8 дБ відповідно) для стеганоповідомлення при забезпеченні високої пропускної спроможності прихованого каналу зв'язку.

В статті [10] наведено теоретичний базис для стеганографічного методу [11], який забезпечує високу надійність вилучення інформації, проте значення PSNR (42 дБ) і пропускна спроможність залишаються недостатньо високими.

Таким чином, аналіз публікацій показав, що для більшості стеганографічних методів характерною є проблема співвідношення якості стеганоповідомлення і пропускної спроможності прихованого каналу зв'язку. Тому метою роботи є розробка стеганографічного методу для цифрових зображень, що забезпечує високу пропускну спроможність прихованого каналу зв'язку при збереженні якості заповненого контейнеру.

Основна частина. Як контейнер будемо розглядати окрему колірну складову цифрового зображення (ЦЗ), представленого в схемі RGB, або полутонове зображення I розміром $M \times N$. В якості додаткової інформації можна використовувати будь-яку бінарну послідовність, сформовану на основі тексту або зображення.

В основі стеганографічного методу лежить теоретичний базис, наведений в [10], основне положення якого полягає в отриманні цілих частотних коефіцієнтів Фур'є для блоків 2×2. Однак стеганографічний метод, розроблений на основі [10], потребує просторової корекції значень яскравості перед обчисленням перетворення Фур'є та передбачає вбудову лише одного біта інформації в блок. Для методу, що розробляється, будемо використовувати швидке перетворення Фур'є для блоку B розміром 2×2:

$$F(u,v) = \sum_{x=0}^{1} \sum_{y=0}^{1} B(x,y) e^{-2i\pi\left(\frac{ux}{2}+\frac{vy}{2}\right)}, \qquad (1)$$

де $F(u,v)$ – (u,v)-й коефіцієнт швидкого перетворення Фур'є, $B(x,y)$ – (x,y)-й піксель блоку B, $u = \overline{0,1}$, $v = \overline{0,1}$.

Вбудову додаткової інформації реалізуємо на основі просторового методу PVD [12] шляхом модифікації різниці між двома коефіцієнтами перетворення Фур'є: $F(0,1)$ і $F(1,0)$. Суть вбудови повідомлення полягає в наступному. З бінарної послідовності вибираються l біт, які переводяться в десяткову систему числення - d. Саме це значення і визначає різницю між пікселями, після чого значення коефіцієнтів модифікуються у відповідності з d.

Коефіцієнти $F(0,1)$ і $F(1,0)$ для вбудови інформації були обрані експериментальним шляхом. При аналізі коефіцієнтів було помічено, що коректне вилучення інформації відбувається лише за умови парних значень абсолютної різниці між коефіцієнтами, що обумовлено тим, що у випадку непарного значення різниці коефіцієнтів обернене перетворення Фур'є призводить до дробових значень яскравості, які потребують округлення до цілих значень. Це в свою чергу веде до некоректної різниці між коефіцієнтами Фур'є при повторному перетворенні. Для уникнення помилок детектування слід подвоювати значення d.

Ще один недолік пов'язаний з широким діапазоном значень абсолютної різниці між коефіцієнтами $F(0,1)$ і $F(1,0)$ для різних блоків. В класичному методі PVD для пікселів ЦЗ це враховується використанням таблиці діапазонів квантування, однак в даному методі через використання подвійних значень d застосування таблиць ускладнене по причині відсутності непарних значень. Тому ми пропонуємо корегувати десяткове значення абсолютної різниці d на величину $s = k \cdot 2^{l+1}$, де $k = \left\lfloor \frac{d}{2^{l+1}} \right\rfloor$, l - число біт, що вбудовуються в блок. Модифікація самих коефіцієнтів відбувається згідно класичного методу PVD [12], після чого виконується обернене швидке перетворення Фур'є:

$$B'(x,y) = \sum_{u=0}^{1}\sum_{v=0}^{1} F'(u,v) e^{2i\pi\left(\frac{ux}{2}+\frac{vy}{2}\right)}, \qquad (2)$$

де $F'(u,v)$ - коефіцієнти Фур'є блоку після вбудови інформації, $B'(x,y)$ - значення яскравості модифікованого блоку, $x = \overline{0,1}$, $y = \overline{0,1}$.

Вилучення додаткової інформації відбувається наступним чином. Для блоку обчислюється швидке перетворення Фур'є, між двома коефіцієнтами $F'(0,1)$ і $F'(1,0)$ обчислюється абсолютне значення різниці d'. Якщо $d' > s$, то модифікуємо значення d' за формулою $d' = d' - s$. Знаходимо $b' = \frac{d'}{2}$, де значення b', переведене у двійкову систему числення, представляє собою фрагмент бінарної послідовності.

Нижче наведені основні кроки вбудови і вилучення повідомлення для запропонованого стеганографічного методу.

Вбудова додаткової інформації в контейнер.

Крок 1. Додаткову інформацію AI представити як бінарну послідовність $binAI$ довжиною L.

Крок 2. Виділити колірну складову I ЦЗ розміром $M \times N$, використовувану для вбудови додаткової інформації AI.

Крок 3. Колірну складову I розбити на блоки B розміром 2×2, що не перетинаються. Для кожного блоку B (кроки 4-10):

Крок 4. Виконати швидке перетворення Фур'є. Результат - B^F.

Крок 5. З послідовності $binAI$ виділити l біт, перевести їх в десяткову систему числення. Результат - b.

Крок 6. Обчислити $d = \left| B_{1,2}^F - B_{2,1}^F \right|$.

Крок 7. Обчислити $b' = 2b + \left\lfloor \frac{d}{2^{l+1}} \right\rfloor \cdot 2^{l+1}$.

Крок 8. Якщо $|b' - d| < |2b - d|$, то $b = b'$, інакше $b = 2b$.

Крок 9. Модифікувати значення $B_{1,2}^F$ і $B_{2,1}^F$ у відповідності до формули

$$\left(B_{1,2}^{F\prime}, B_{2,1}^{F\prime}\right)=\begin{cases}\left(B_{1,2}^{F}+\left\lceil\frac{m}{2}\right\rceil, B_{2,1}^{F}-\left\lfloor\frac{m}{2}\right\rfloor\right), \text{якщо } B_{1,2}^{F}\geq B_{2,1}^{F} \,\&\, b>d\\ \left(B_{1,2}^{F}-\left\lfloor\frac{m}{2}\right\rfloor, B_{2,1}^{F}+\left\lceil\frac{m}{2}\right\rceil\right), \text{якщо } B_{1,2}^{F}< B_{2,1}^{F} \,\&\, b>d\\ \left(B_{1,2}^{F}-\left\lceil\frac{m}{2}\right\rceil, B_{2,1}^{F}+\left\lfloor\frac{m}{2}\right\rfloor\right), \text{якщо } B_{1,2}^{F}\geq B_{2,1}^{F} \,\&\, b\leq d\\ \left(B_{1,2}^{F}+\left\lceil\frac{m}{2}\right\rceil, B_{2,1}^{F}-\left\lfloor\frac{m}{2}\right\rfloor\right), \text{якщо } B_{1,2}^{F}< B_{2,1}^{F} \,\&\, b\leq d\end{cases}$$

де $m=|b-d|, \lfloor\bullet\rfloor$ - округлення до найменшого цілого, $\lceil\bullet\rceil$ - округлення до найбільшого цілого.

Крок 10. Виконати обернене швидке перетворення Фур'є. Результат - B'.

Крок 11. Зберегти заповнений контейнер.

Вилучення додаткової інформації з заповненого контейнеру.

Крок 1. Виділити колірну складову I' ЦЗ розміром $M\times N$, яка містить додаткову інформацію.

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

Для кожного блоку B' (кроки 3-6):

Крок 3. Виконати швидке перетворення Фур'є. Результат - $B^{F\prime}$.

Крок 4. Обчислити $d'=\left|B_{1,2}^{F\prime}-B_{2,1}^{F\prime}\right|$.

Крок 5. Якщо $d'\geq\left\lfloor\frac{d'}{2^{l+1}}\right\rfloor\cdot 2^{l+1}$, то $b'=\frac{d'-\left\lfloor\frac{d'}{2^{l+1}}\right\rfloor\cdot 2^{l+1}}{2}$, інакше $b'=\frac{d'}{2}$.

Крок 6. Перевести значення b' в двійкову систему числення довжиною l біт. Додати отримане значення до бінарної послідовності AI'.

Крок 7. З бінарної послідовності AI' сформувати вилучене повідомлення.

Ефективність розробленого стеганографічного методу будемо оцінювати на основі наступних показників:

- PSNR, що визначає якість заповненого контейнеру у порівнянні з оригінальним ЦЗ;
- NCC [13], що визначає точність вилучення вбудованого повідомлення;
- пропускної спроможності прихованого каналу зв'язку.

Пропускна спроможність прихованого каналу зв'язку розраховується як число біт вбудованого повідомлення на один елемент контейнера. Для запропонованого методу максимальна ємність колірної складової I розміром $M\times N$ оцінюється як

$$v=\left\lfloor\frac{M}{2}\right\rfloor\cdot\left\lfloor\frac{N}{2}\right\rfloor\cdot l,$$

де l - число біт повідомлення, вбудованих в один блок 2×2 ЦЗ.

Пропускна спроможність обчислюється за формулою

$$capacity=\frac{v}{MN}.$$

Відповідно, вбудовуючи 4 біти повідомлення в кожний блок пропускна спроможність буде становити 1 біт/піксель, а при вбудові 3 біт повідомлення – 0,75 біт/піксель. Порівнюючи пропускну спроможність з роботами [7, 11], в яких пропускна спроможність складає 0,7 і 0,25 біт/піксель відповідно), розроблений метод забезпечує високу пропускну спроможність прихованого каналу зв'язку.

Для оцінки якості стеганоповідомлень та якості вилучення додаткової інформації був проведений обчислювальний експеримент на основі 200 цифрових зображень різного розміру. В якості вбудованого повідомлення в експерименті були використані напівтонові ЦЗ. В таблиці 1 наведені середні значення показників PSNR та NCC, а також максимальні і мінімальні значення NCC для наступних випадків:

– в кожний блок синьої колірної складової відбувалась вбудова 4-х біт повідомлення (експеримент 1);

– в кожний блок синьої колірної складової відбувалась вбудова 3-х біт повідомлення (експеримент 2);

– в кожний блок зеленої колірної складової відбувалась вбудова 3-х біт повідомлення (експеримент 3).

У всіх трьох експериментах заповнені контейнери були збережені без втрат.

Таблиця 1

Ефективність вилучення додаткової інформації із заповненого контейнеру

	Середнє значення PSNR, дБ	Середнє значення NCC	Максимальне значення NCC	Мінімальне значення NCC
Експеримент 1	58,633282	0,87922645	0,99989	0,2648
Експеримент 2	60,076282	0,9373597	0,9996	0,41737
Експеримент 3	60,024235	0,9721804	0,99994	0,80379

З таблиці 1 видно, що при забезпеченні високої пропускної спроможності прихованого каналу зв'язку (1 і 0,75 біт/піксель) забезпечуються високі показники PSNR порівняння оригінального контейнеру і отриманого стеганоповідомлення – середні значення становлять від 58 до 60 дБ. Однак точність вилучення додаткової інформації при використанні синьої колірної складової контейнеру недостатньо висока – середні значення показника NCC становлять 0,87-0,94 через наявність таких стеганоповідомлень, з яких вилучена додаткова інформація дуже відрізняється від вбудованої, про що свідчать дуже низькі мінімальні значення NCC в експериментах 1 і 2. При вбудові 4-х біт в кожний блок погане вилучення повідомлення (NCC менше 0,7) відбувалося в 12,5% заповнених контейнерів, зменшення кількості біт дозволило зменшити долю стеганоповідомлень з поганим вилученням інформації до 5%.

Аналіз причин некоректного вилучення повідомлення показав, що синя колірна складова містить багато блоків зі значеннями яскравості, близьких до 0 та 255, набагато більше, ніж в червоній і зеленій колірних складових. Модифікація коефіцієнтів Фур'є таких блоків призводить до того, що в результаті оберненого перетворення Фур'є ми отримуємо значення яскравостей, менших нуля або більших 255, що призводить до округлень до граничних значень – 0 або 255. В результаті при вилученні інформації виникають помилки. Нижче наведено приклад некоректного вилучення додаткової інформації:

$$\begin{pmatrix}4 & 0\\ 1 & 1\end{pmatrix}\xrightarrow{fft2}\begin{pmatrix}6 & 4\\ 2 & 4\end{pmatrix}\xrightarrow{вбудова\ 3=011_2}\begin{pmatrix}6 & 6\\ 0 & 4\end{pmatrix}\xrightarrow{ifft2}\begin{pmatrix}4 & -1\\ 2 & 1\end{pmatrix}\to\begin{pmatrix}4 & 0\\ 2 & 1\end{pmatrix},$$

$$\begin{pmatrix}4 & 0\\ 2 & 1\end{pmatrix}\xrightarrow{fft2}\begin{pmatrix}7 & 5\\ 1 & 3\end{pmatrix}\xrightarrow{вилучення}|5-1|=4\to\frac{4}{2}=2=010_2.$$

Для порівняння ефективності вилучення повідомлення, вбудованого в іншу колірну складову, був проведений експеримент вбудови 3-х біт додаткової інформації в кожний блок зеленої колірної складової ЦЗ (експеримент 3). В таблиці 1 видно, що результати вилучення повідомлення в експерименті 3 набагато краще результатів експерименту 2 – середнє значення NCC становить 0,97, а мінімальне – 0,8. Тому для забезпечення високої точності вилучення додаткової інформації рекомендується проводити аналіз матриць ЦЗ та обирати ту з них, яка містить найменшу кількість блоків зі значеннями, близькими до 0 або 255.

Для оцінки стійкості запропонованого методу до атак зашумленням був проведений обчислювальний експеримент, результати якого наведені в таблиці 2.

Таблиця 2

Ефективність вилучення додаткової інформації із заповненого контейнеру після атак

Атака	Параметри	Середнє значення PSNR, дБ	Середнє значення NCC	Максимальне значення NCC	Мінімальне значення NCC
Експеримент 1					
Гаусів шум	$m=0, d=0.00001$	48,86962	0,344633	0,44853	0,061157
	$m=0, d=0.000001$	56,36327	0,802141	0,91876	0,24327
Мультиплі-кативний шум	$d=0.00005$	49,40806	0,539976	0,98263	0,093479
	$d=0.000006$	55,32855	0,787686	0,99989	0,18039
	$d=0.000001$	58,63328	0,879226	0,99989	0,2648
Шум «Сіль та перець»	$d=0.01$	24,6721	0,861752	0,97989	0,25954
	$d=0.005$	26,582	0,870476	0,9901	0,26237
Експеримент 2					
Гаусів шум	$m=0, d=0.00001$	49,14321	0,288482	0,33804	0,19205
	$m=0, d=0.000001$	57,49274	0,841496	0,89902	0,38408
Мультиплі-кативний шум	$d=0.00005$	49,03103	0,476161	0,88556	0,16396
	$d=0.000006$	56,01979	0,810879	0,9982	0,29988
	$d=0.000001$	60,07628	0,93736	0,9996	0,41737
Шум «Сіль та перець»	$d=0.01$	24,92572	0,918699	0,98018	0,40956
	$d=0.005$	27,93963	0,928015	0,99017	0,41289
Експеримент 3					
Гаусів шум	$m=0, d=0.00001$	49,13999	0,296112	0,34005	0,24478
	$m=0, d=0.000001$	57,46723	0,872095	0,90179	0,72341
Мультиплі-кативний шум	$d=0.00005$	49,02722	0,417405	0,90854	0,17678
	$d=0.000006$	56,00131	0,823811	0,99655	0,49959
	$d=0.000001$	60,02424	0,97218	0,99994	0,80379
Шум «Сіль та перець»	$d=0.01$	24,92548	0,952747	0,97987	0,78745
	$d=0.005$	27,93351	0,962455	0,99	0,79591

З табл. 2 видно, що найгірші результати вилучення повідомлення спостерігаються при помітному зашумленні Гаусовим і мультиплікативним шумами ($m=0, d=0.00001$ і $d=0.00005$ відповідно) – у всіх експериментах спостерігаються низькі значення показника NCC, однак при менших спотвореннях стеганоповідомлення забезпечується досить висока якість вилучення додаткової інформації – середні значення NCC дорівнюють від 0,78 до 0,94. Окремо слід відзначити стійкість запропонованого методу до атаки шумом «Сіль та перець» - навіть при великих спотвореннях заповненого контейнеру (про що свідчать низькі значення PSNR від 24 до 27 дБ) точність вилучення повідомлення з синьої колірної складової при різних

значеннях пропускної спроможності становить від 0,86 до 0,93, а при вилученні з зеленої колірної матриці – 0,95-0,96.

На рис. 1 наведений приклад вбудови додаткової інформації (рис.1, г) в зелену колірну складову контейнеру (рис.1, а) з пропускною спроможністю 0,75 біт/піксель, а також результатів вилучення повідомлень (рис.1, д, е) з заповнених контейнерів (рис.1, б, в). Стеганоповідомлення, наведене на рис.1, в, зазнало атаки шумом «Сіль та перець» з дисперсією $d = 0.03$, що призвело до помітних спотворень зображення, однак секретна інформація вилучена з нього з високою точністю (рис.1, е), хоч і має деякі завади у вигляді чорних і білих точок.

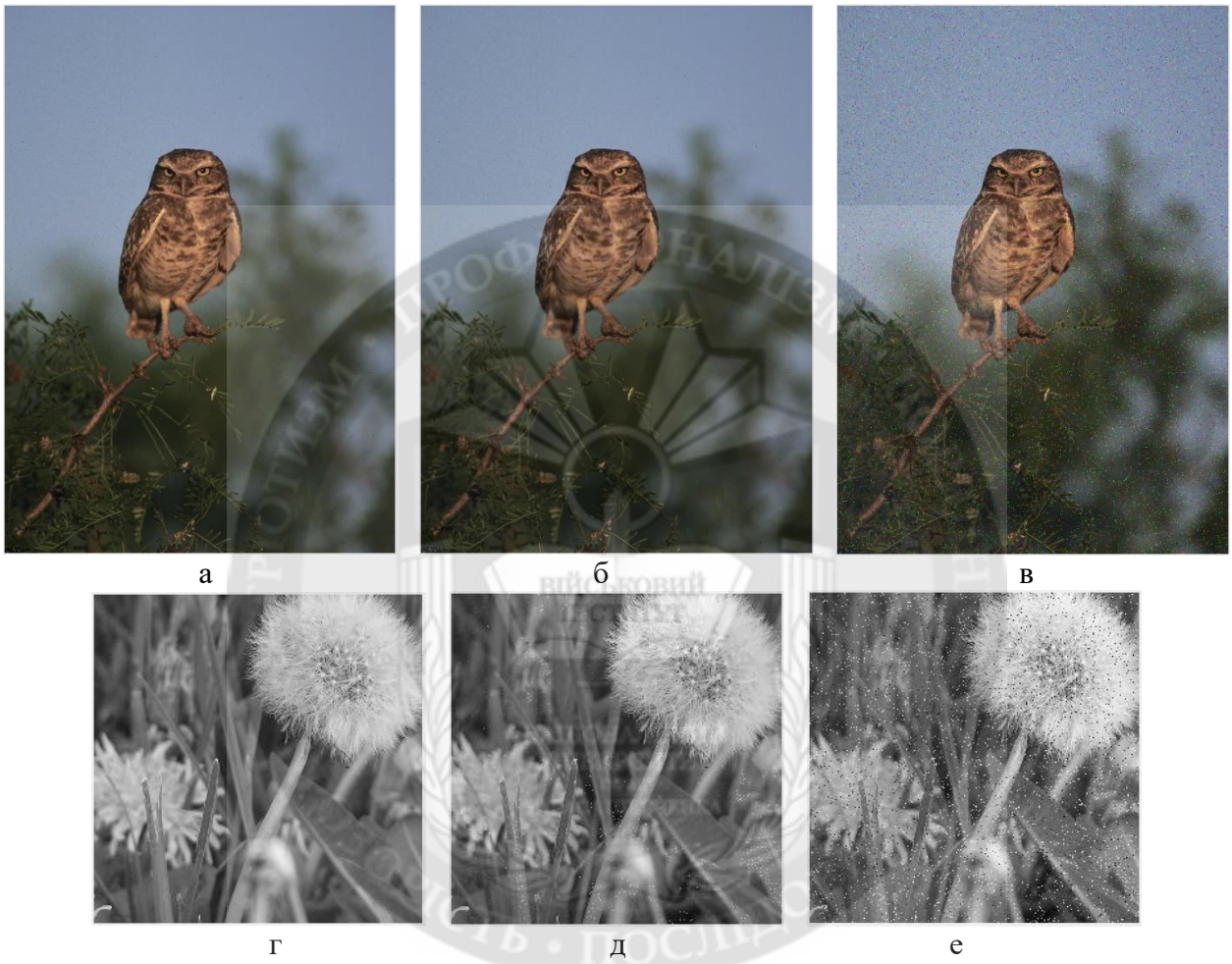

Рисунок 1 – Результати вилучення додаткової інформації: а – контейнер; б – стеганоповідомлення (PSNR=58,5642 дБ); в – стеганоповідомлення після атаки шумом «Сіль та перець» при $d = 0.03$ (PSNR=20,4152 дБ); г – оригінальна додаткова інформація; д – повідомлення, вилучене з заповненого контейнеру без атак (NCC=0,98757); е – повідомлення, вилучене з заповненого контейнеру після атаки шумом «Сіль та перець» (NCC=0,92871)

Висновки. В статті запропонований новий стеганографічний метод для цифрових зображень на основі швидкого перетворення Фур'є. Вбудова додаткової інформації відбувається в блоки 2×2 шляхом модифікації різниці між двома коефіцієнтами перетворення Фур'є. В кожний блок можна вбудувати до чотирьох біт повідомлення, що дозволяє забезпечити високу пропускну спроможність прихованого каналу зв'язку при збереженні високої якості стеганоповідомлення (середнє значення PSNR становить 58-60 дБ).

В ході проведених обчислювальних експериментів встановлено, що в більшості випадків забезпечується висока точність вилучення додаткової інформації (в 88% заповнених контейнерів з усіх експериментів показник NCC перевищує значення 0,9), однак при використанні синьої колірної складової спостерігаються досить високі помилки, пов'язані з характеристиками самого контейнеру, а саме наявністю великої кількості блоків зі значеннями яскравості, близькими до 0 або 255. Мінімізувати помилки вилучення повідомлення можна шляхом вибору тієї колірної складової, яка містить якомога менше таких блоків.
Експерименти, спрямовані на аналіз стійкості до атак, зокрема зашумлення, показали високу стійкість до шуму «Сіль та перець», а також до Гаусового та мультиплікативних шумів при незначних спотвореннях стеганоповідомлень.

ЛІТЕРАТУРА:

1. Arup Kumar Pal. A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity / Arup Kumar Pal, Kshiramani Naik, Rohit Agarwa // The International Arab Journal of Information Technology. – 2019. – Vol. 16. – No. 1. – pp.116-124.

2. Saidi, M. A new adaptive image steganography scheme based on DCT and chaotic map. / Saidi, M., Hermassi, H., Rhouma, R. // Multimedia Tools and Applications. – 2017. – No. 76. – Pp. 13493-13510.

3. Safwat Hamad. A Blind High-Capacity Wavelet-Based Steganography Technique for Hiding Images into other Images / Safwat Hamad, Amal Khalifa, Ahmed Elhadad // Advances in Electrical and Computer Engineering. – 2014. – Volume 14. – Number 2. – Pp.35-42.

4. Kumar, V. A modified DWT-based image steganography technique / Kumar, V., Kumar, D. // Multimedia Tools and Applications. – 2018. – No. 77. – Pp.13279–13308.

5. 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.

6. 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.

7. Khalil M.I. Using Quaternion Fourier Transform in Steganography Systems / M.I. Khalil // International Journal of Communication Networks and Information Security. – 2018. – Vol. 10. – No. 2. – Pp.425-431.

8. Nabin Ghoshal. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT) / Nabin Ghoshal, J. K. Mandal // Proceedings of ICCS, 2010, November 19-20. – Pp.144-150.

9. Ashish Soni. Image Steganography using Discrete Fractional Fourier Transform / Ashish Soni, Jitendra Jain, Rakesh Roshan // International Conference on Intelligent Systems and Signal Processing (ISSP2013), India. – Pp.99-103.

10.Kozina M.O. Discrete Fourier Transform As A Basis For Steganographic Method / M.O. Kozina // Праці Одеського політехнічного університету. – 2014. – Вип. 2(44). – С.147-154.

11.Козина М.А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации / М.А. Козина // Сучасна спеціальна техніка. – 2014. - № 4(39). – С.98-106.

12.Wu D.C. A Steganographic method for images by pixel-value differencing / D.C. Wu, W.H. Tsai // Pattern Recognition Letters. – 2003. - Vol. 24. - Pp. 1613-1626.

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. Arup Kumar Pal1, Kshiramani Naik1, and Rohit Agarwal (2019), "A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity", The International Arab Journal of Information Technology, Vol. 16, No. 1, pp.116-124.

2. Saidi, M., Hermassi, H., Rhouma, R. (2017), "A new adaptive image steganography scheme based on DCT and chaotic map", Multimedia Tools and Applications, No. 76, pp. 13493-13510.

3. Safwat Hamad, Amal Khalifa, Ahmed Elhadad, (2014), “A Blind High-Capacity Wavelet-Based Steganography Technique for Hiding Images into other Images”, Advances in Electrical and Computer Engineering, Volume 14, Number 2, pp.35-42.

4. Kumar, V., Kumar, D. (2018) “A modified DWT-based image steganography technique”, Multimedia Tools and Applications, No. 77, pp.13279–13308.

5. 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.

6. 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.

7. Khalil M.I. (2018) “Using Quaternion Fourier Transform in Steganography Systems”, International Journal of Communication Networks and Information Security, Vol. 10, No. 2, pp.425-431.

8. Nabin Ghoshal (2010) “Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT)”, Proceedings of ICCS, 2010, November 19-20, pp.144-150.

9. Ashish Soni (2013) “Image Steganography using Discrete Fractional Fourier Transform”, International Conference on Intelligent Systems and Signal Processing (ISSP2013), India, pp.99-103.

10.Kozina M.O. (2014) Discrete Fourier Transform As A Basis For Steganographic Method, Pratsi Odes′koho politekhnichnoho universytetu [Proceedings of Odessa Polytechnic University], Iss. 2(44), pp.147-154.

11.Kozina M.A. (2014) “Steganographic method of organizing a hidden communication channel, checking the integrity of the transmitted information”, Suchasna spetsial′na tekhnika [Modern special equipment], № 4 (39), pp.98-106.

12.Wu D.C., W.H. Tsai. (2003) “A Steganographic method for images by pixel-value differencing”, Pattern Recognition Letters, Vol. 24, pp.1613-1626.

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., Bezsonova M.D.

DEVELOPMENT OF A STEGANOGRAPHIC METHOD FOR DIGITAL IMAGES BASED ON FOURIER TRANSFORM

In the modern Internet space in conditions of continuous exchange of information the need to protect it from the possibility of unauthorized use by third parties is increasing. This can be ensured by using steganographic methods that allow organizing a covert communication channel.

In the article a new steganographic method for digital images based on the fast Fourier transform developed. As additional information you can use both text messages and images translated into a binary sequence. For embedding of additional information 2×2 blocks are used for which the fast Fourier transform is calculated. Message embedding is done by modifying the absolute difference between two coefficients of block’s Fourier transform. Up to four bits of a binary sequence can be embedded in each block.

The results of computational experiments aimed at assessing the effectiveness of the proposed method have shown that high quality of stegos is provided (average PSNR values are 58-60 dB) compared to modern analogues while ensuring high capacity of the covert communication channel (0.75 and 1 bit/pixel). The average values of the extraction accuracy index of additional information NCC are from 0.87 to 0.97 depending on the selected color component and the number of embedded bits. The accuracy of message extraction depends on the characteristics of the container - detection errors occur when there are a large number of blocks with brightness values close to 0 or 255. However, this problem can be eliminated by preliminary analysis of the container.

The developed method showed high resistance to attack by the noise "Salt and pepper" (d=0.01) at appreciable distortions of the filled container, as well as the imposition of a Gaussian and a multiplicative noise at imperceptible distortions of stegos.

Keywords: steganography, fast Fourier transform, digital image.