УДК 519.6

О.М. ЛИТВИН, д-р фіз.-мат. наук, проф., УІПА, Харків
А.І. ДРОБОТЯ, канд. техн. наук, доц. БДПУ, Бердянськ
С.І. КУЛИК, канд. фіз.-мат. наук, ст. викладач НТУ «ХПІ», Харків
О.О. ЛИТВИН, канд. фіз.-мат. наук, ст. наук. співробітник., УІПА, Харків

СТВОРЕННЯ ГРАФІЧНОГО СТЕГОФАЙЛУ НА ЗОБРАЖЕННІ-КОНТЕЙНЕРІ З ВИКОРИСТАННЯМ ВЕЙВЛЕТІВ

В статті запропоновано метод створення графічного стегоповідомлення на основі статичного зображення та вейвлетів. На конкретному прикладі (передача секретного графічного повідомлення) розглянуто роботу розробленого алгоритму, наведено результати роботи програми та аналіз результатів проведеного обчислювального експерименту. Також розглянуто перспективи подальших досліджень.

The article suggests a method of creating graphical steganomessage based on static images, and wavelets. In a specific example (transmission of the confidential picture message), we reviewed the work of the algorithm, cited the results of the program and quoted the analysis results of the experiments. Also we consider some recommendations for further research.

1. Вступ. Використання зображень, звукових чи відео-файлів в ролі контейнерів для передачі стегоповідомлення відкриває досить широкі можливості з огляду на значний об'єм наявної інформації.

2. Аналіз останніх досліджень. Незначна змінюваність первинних образів після "вживлення" стегоповідомлення, що не провокує підозр щодо наявності в них сторонньої інформації розглядалася в роботах [1-3]. Ідеальними для такої ролі є зображення, оскільки вони вже піддані стисненню, достатньо великі за обсягом і добре скривають конфіденційну інформацію [4-5]. Якщо стеганографічна процедура виконує свою роботу добре, розходження в рівневі якості зображення після змін, які відбулися для того, щоб сховати повідомлення, не привернуть увагу стороннього спостерігача. Враховуючи викладене вище, актуальною є задача побудови технологічно зручної процедури вживлення секретної графічної інформації в інформацію зображення-контейнера та вилучення його звідти.

3. Постановка задачі. Зображення мають значні переваги перед іншими носіями в ролі контейнерів [5]. Задача шифрування полягає у непомітному вкрапленні конфіденційної інформації шляхом застосування вейвлет-перетворення до матриці зображення-контейнера як функції двох змінних $f(x,y)$ та «приклеюванні» цілочислових значень інтенсивності білого кольору (або інших значень) у кожному пікселі прихованого графічного повідомлення до мантиси обраного вейвлет-коефіцієнта і подальшому застосуванні оберненого вейвлет-перетворення до матриці «спотворених» вейвлет-коефіцієнтів.

Задача дешифрування полягає у вилученні цілочислових значень інтенсивності білого кольору у кожному пікселі зашифрованого повідомлення шляхом застосування прямого вейвлет-перетворення отриманої матриці «спотвореного» зображення та порівняння з матрицею вейвлет-перетворення використовуваного еталонного зображення. Слід підкреслити, що розміри зображення-контейнера не перевищують розмірів зображення секретного графічного повідомлення. Якщо ж зображення-контейнер має більші розміри ніж саме приховане повідомлення, то вибір послідовності коефіцієнтів матриці вейвлет-перетворення для «приклеювання» надає досить широкі можливості додаткового ускладнення ситуації проти спроб атаки стегоповідомлення. Окремим випадком є ситуація, коли розміри зображення-контейнера є меншими, ніж розміри зображення-повідомлення. В цьому разі з'являється можливість додаткового ускладнення атаки на стегофайл, якщо створити додатковий алгоритм «стиснення» прихованого графічного повідомлення. Залишаємо поза обговоренням те, що саме графічне повідомлення може бути оброблено якимось криптографічним алгоритмом [6] або попередньо піддане якомусь іншому вейвлет-перетворенню.

4. Основні результати. Перейдемо до особи, яка передає секретне графічне повідомлення. Отже, будемо розглядати підготовче перетворення еталонного зображення для створення файлу-контейнера використовуючи вейвлет-перетворення Добеші четвертого порядку. Викладемо етапи роботи алгоритму за кроками, обмежуючись лише зображенням у «градаціях сірого». Безумовно, використання повної гами кольорів надає додаткові можливості захисту конфіденційного повідомлення, запобігаючи успішність атаки на стего-файл. Наприклад, зображення у стандартах RGB або CMY мають три складники, за рахунок яких можна поглибити рівень шифрування або збільшити розмір повідомлення, що підлягає передачі.

Нехай еталонне зображення містить $M \times N$ точок-пікселів. Зручно вибрати розмір так, щоб кожне з чисел M та N було степенем двійки ($M = 2^p$, $N = 2^q$). Тоді зображення можна подати у вигляді матриці, елементи якої $f(x, y)$, $x = \overline{0, M-1}$, $y = \overline{0, N-1}$ - значення функції двох змінних є інтенсивності білого кольору, числові значення якої в межах від 0 до 255. Слід зауважити, що в системі комп'ютерної математики (СКМ) MathCad зображення можна подати у вигляді матриці $A_{i \times j}$, $i = \overline{0, M-1}$, $j = \overline{0, N-1}$, кожен елемент a_{ij} якої містить згадуване значення інтенсивності білого. Таким чином, робота із функцією $f(x, y)$ в системі комп'ютерної математики MathCad зводиться до роботи з матрицею A. На рис. 1 бачимо еталонне зображення «Lena» (512× 512 пікселів) та матрицю L, що йому відповідає.

L =

	0	1	2	3	4	5	6	7	8	9
0	162	162	162	161	162	157	163	161	166	162
1	162	162	162	161	162	157	163	161	166	162
2	162	162	162	161	162	157	163	161	166	162
3	162	162	162	161	162	157	163	161	166	162
4	162	162	162	161	162	157	163	161	166	162
5	164	164	158	155	161	159	159	160	161	160
6	160	160	163	158	160	162	159	156	159	163
7	159	159	155	157	158	159	156	157	159	162
8	155	155	158	158	159	160	157	157	163	157
9	155	155	157	158	155	154	155	157	161	155
10	156	156	156	160	156	155	155	152	159	159
11	156	156	156	159	159	155	150	148	160	159
12	158	158	157	156	157	153	159	156	161	158
13	157	157	157	157	160	157	156	156	159	155
14	158	158	159	155	155	158	158	156	157	156
15	158	158	159	157	155	158	157	154	158	158

L

Рисунок 1 – Еталонне зображення «Lena» та матриця, що йому відповідає.

Відмітимо загальновідомий факт, що у 1987 Інгрид Добеші сконструювала ортонормований базис вейвлетів, що залишається ключовим і сьогодні для багатьох вейвлет-додатків [7].

Для створення стегофайлу з прихованим повідомленням потрібно виконати таку послідовність дій.

1. Попередня обробка зображення полягає у застосуванні двовимірного вейвлет-перетворення Добеші четвертого порядку W до функції $f(x,y)$, яка відповіає матриці L. Отримаємо

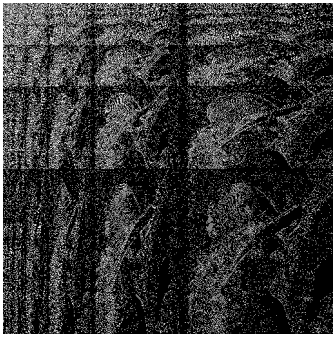
$$f'(x,y) = W\left[f(x,y)\right], \text{ або } f(x,y) \xrightarrow{W} f'(x,y).$$

В пакеті MathCAD вейвлет-перетворення Добеші четвертого порядку представлено функціями ***wave*** та ***iwave*** – відповідно пряме та обернене перетворення. Причому аргументами даних функцій повинні бути дійсні числа, а їх кількість повинна дорівнювати 2^m, де m – ціле число. Оскільки аргументом функцій ***wave*** та ***iwave*** є вектор-стовпчик або вектор-рядок даних, то обробка (двовимірне вейвлет-перетворення) всього зображення відбувається за рядками, а потім за стовпчиками – почергово. В результаті отримаємо матрицю коефіцієнтів вейвлет-перетворення Добеші $A'_{i\times j}$ тієї ж вимірності та розміру, що і початкове зображення. На рис.2 бачимо матрицю PP отриманих вейвлет-коефіцієнтів Добеші та зображення, що їй відповідає.

2. Підготовлене певне зображення X (відповідає функції $z(x,y)$), яке підлягає передачі в умовах конфіденційності може містити кількість пікселів не більшу, ніж кількість коефіцієнтів матриці (інші можливі випадки обговорювались вище). Воно може бути, безумовно, попередньо закодоване якимось з криптоалгоритмів або стиснуте тощо. Основними вимогами до таких «перетворень», що виконуються над прихованим зображенням, є наступні: по-перше, результат застосування такого перетворення (прямого і

PP =

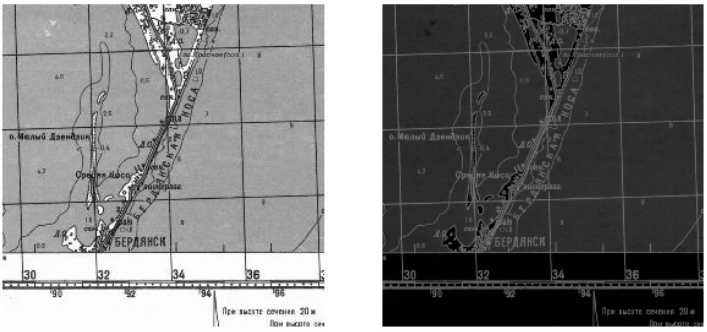
	0	1	2
0	32303.1969654389	33406.3869510251	-2190.87693360257
1	27765.3892149918	33552.6987435441	-3572.11667124146
2	5052.34154727903	-1693.21283446563	-1436.14229764542
3	-2709.39288649274	1597.94799814568	-22.9987701658558
4	446.936774257886	121.358247993831	1368.08334300313
5	885.89290480263	1728.63744213491	177.885593661272
6	447.5963010323	-81.7814902798186	-1243.12926729109
7	-600.975683771808	561.626504950556	-285.919808996274
8	200.516958490733	1061.63902225991	780.698714364885
9	93.3408951083257	-1281.74815154822	-74.2194214826491
10	1079.73811367982	1107.50313158297	-974.757134304225
11	-697.436430939079	6.77743454508286	659.712310221857
12	74.0734939022542	-532.666632078289	45.0665883419464
13	466.099339931431	451.789665624498	-436.153172378604
14	-94.8346787613225	-766.661771080127	569.10781705403
15	-502.88250430985	-280.990857988019	-276.218359924434



$\frac{PP}{7}$

Рисунок 2 – Матриця отриманих вейвлет-коефіцієнтів Добеші та відповідне їй зображення.

йому оберненого) не повинен істотно змінювати приховане повідомлення, тобо має бути перетворенням «без втрат»; по-друге, в результі застосування такого прямого перетворення матриця зображення прихованого повідомлення повинна перетворитись на таку, що містить числа, які складаються із невеликої кількості цифр (бажано не більше трьох). Це дозволяє позбутися запису надлишкової інформації до зображення-контейнера і, таким чином, вносить мінімальні спотворення до сформованого стегофайлу. Не порушуючи загальності, і для простоти викладу виконаємо наступне перетворення P матриці секретного зображення. Оскільки матриця прихованого зображення містить переважно елементи більші ніж 150 (відповідає світло-сіріому), змінимо ці заначення на менші, віднявши їх значення від максимального (255) і поділивши результат на 2. Такими діями ми досягли зменшення значень елементів матриці прихованого зображення. На рисунку 3 бачимо секретне зображення X і його аналог Xp після виконання перетворення.



X Xp

Рисунок 3 – Приховане графічне повідомлення X – задане спочатку і після застосування перетворення P – Xp .

3. На третьому етапові виконуємо «приклеювання» елементів перетвореної матриці Xp секретного графічного повідомлення X до коефіцієнтів Добеші матриці PP (відповідає функції $f'(x,y)$) перетвореного зображення-контейнера, шляхом звичайного додавання цих матриць. З метою усунення значного спотворення зображення, внаслідок зміни коефіцієнтів Добеші, «приклеювати» (додавати) числа, що є кодами символів приховуваного повідомлення, будемо до мантиси коефіцієнтів (наприклад, починаючи з 9 знаку після коми). Позначимо через d функцію домовленості, яка визначає розташування «приклеюваних» елементів перетвореної матриці Xp секретного графічного повідомлення X до коефіцієнтів Добеші. Можливості варіювати «приклеювання» досить широкі: можна починати додавання за елементами діагоналей, за рядками чи стовпчиками, випадковим чином, за домовленим порядком тощо. Функція d може бути, наприклад, функцією, що залежить від часу. В результаті отримаємо:

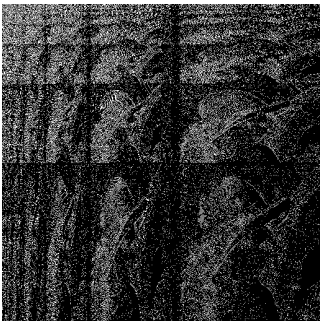
$$g(x,y) = f'(x,y) + S(x,y), \qquad (1)$$

де $S(x,y) = d\left[z'(x,y)\right]$, $z'(x,y) = P\left[z(x,y)\right]$, або $z(x,y) \xrightarrow{P} z'(x,y)$.

Для спрощення теоретичних викладок, але не порушуючи загальності, в нашому прикладі, додамо елементи перетвореної матриці секретного графічного повідомлення до відповідних елементів матриці коефіцієнтів вейвлет-перетворення зображення-контейнера (рис. 4).

PPzminen=

	0	1	2
0	32303.1969656029	33406.3869511891	-2190.87693343957
1	27765.3892151558	33552.6987437081	-3572.11667107846
2	5052.34154743603	-1693.21283430563	-1436.14229748242
3	-2709.39288634274	1597.94799830168	-22.9987700028558
4	446.936774414886	121.358248153831	1368.08334316613
5	885.89290495963	1728.63744229391	177.885593822272
6	447.5963011943	-81.7814901168186	-1243.12926712809
7	-600.975683604808	561.626505117556	-285.919808829274
8	200.516958655733	1061.63902242391	780.698714528885
9	93.3408952683257	-1281.74815139022	-74.2194213256491
10	1079.73811384182	1107.50313174197	-974.757134147225
11	-697.436430770079	6.77743471008286	659.712310383857
12	74.0734940782542	-532.666631908289	45.0665885069464
13	466.099340105431	451.789665792498	-436.153172214604
14	-94.8346785923225	-766.661770915127	569.10781721603
15	-502.88250414485	-280.990857826019	-276.218359764434



$\frac{PPzminen}{7}$

Рисунок 4 – Матриця PPzminen і відповідне їй зображення змінених вейвлет-коефіцієнтів.

4. Четвертий етап полягає у відтворенні «спотвореного» зображення. Звідси зрозуміло, що зображення мусить бути достатньо різноманітним у деталях. «Спотворене» зображення отримуємо шляхом застосування оберненого вейвлет-перетворення IW до вже змінених сторонньою (прихованою) інформацією коефіцієнтів Добеші $g(x,y)$.

$$\bar{g}(x,y) = IW\left[g(x,y)\right] \text{ або } g(x,y) \xrightarrow{IW} \bar{g}(x,y).$$

На рис. 5 наведено еталонне зображення L і «спотворене» зображення Q. Залишається передати «спотворене» зображення Q з повідомленням (відповідає функції $\bar{g}(x,y)$) адресатові.

L Q

Рисунок 5 – Візуальне порівняння еталонного зображення L і «спотвореного» зображення Q.

Як бачимо, еталонне і «спотворене» зображення візуально не відрізняються. Отже, у стороннього спостерігача не виникне підозр щодо наявності у зображенні прихованої інформації.

5.Далі відбувається передача сформованого стегофайлу Q адресатові, який має еталонне зображення L або серію (добірку) таких зображень, які вибираються за певною домовленістю; має функцію d та знає алгоритм дешифрування (обернене перетворення IP) графічного стегоповідомлення.

Для вилучення секретного повідомлення адресатові належить виконати послідовність таких дій:

1. Вибрати відповідне еталонне зображення $f(x,y)$ з набору.

2. Виконати пряме вейвлет-перетворення Добеші еталонного зображення та отриманого стегофайлу, діставши

$$f'(x,y) = Wf(x,y) \text{ або } f(x,y) \xrightarrow{W} f'(x,y),$$

$$g(x,y) = W\bar{g}(x,y) \text{ або } \bar{g}(x,y) \xrightarrow{W} g(x,y).$$

3. Порівняти функції $g(x,y)$ та $f'(x,y)$. Тобто, маючи $g(x,y)$ та $f'(x,y)$, з рівності (1) отримаємо функцію $S(x,y)$, що містить приховану інформацію, яка розміщена у певному порядку d:

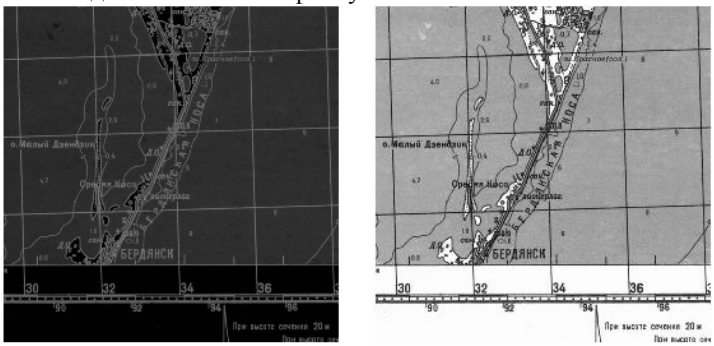
$$S(x,y) = g(x,y) - f'(x,y).$$

4. Знаючи функцію d, вилучити змінене секретне графічне повідомлення $z(x,y)$ здійснивши зворотні дії:

$$z'(x,y) = d^{-1}\left[S(x,y)\right], \qquad (2)$$

$$z(x,y) = IP\left[z'(x,y)\right] \text{ або } z'(x,y) \xrightarrow{IP} z(x,y). \qquad (3)$$

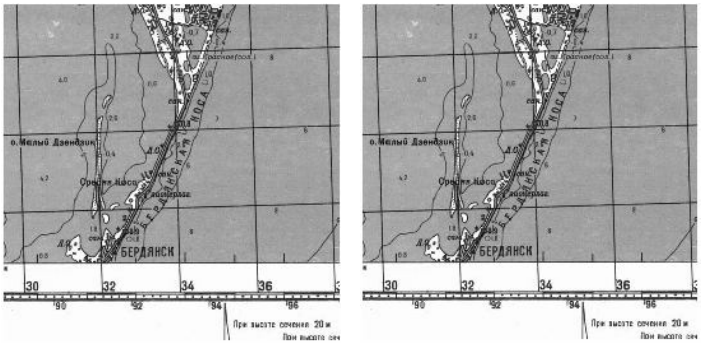
На рис.6 показано успішний результат роботи програми з вилучення графічного повідомлення із стегофайлу.



Riznytsya 255 – Riznytsya-2

Рисунок 6 – Результат роботи програми з вилучення прихованого графічного повідомлення із отриманого стегофайлу відповідно до формули (2) і формули (3).

На рис.7 для візуального порівняння наведено результат, отриманий в ході роботи програми дешифрування і оригінал секретного графічного повідомлення, що вводився на початку програми зі створення графічного стегофайлу.



255 – Riznytsya-2 X

Рисунок 7 – Візуальне порівняння результату роботи програми з вилучення прихованого графічного повідомлення із отриманого стегофайлу (зліва) і оригінала секретного графічного повідомлення (справа).

5. Висновки. Таким чином, у даній роботі успішно реалізовано алгоритм створення стегофайлу на стандартному зображенні-контейнері – «Lena», що представлене у «градаціях сірого» з використанням вейвлетів Добеші 4 порядку. Про це свідчить візуальне порівняння еталонного зображення L і зображення Q отриманого стегофайлу – рис. 5. А також успішно реалізовано алгоритм вилучення секретного графічного повідомлення із отриманого зображення – стегофайлу Q, про що свідчить візуальне порівняння результату роботи програми дешифрування (зображення « $255 - Riznytsya \cdot 2$ ») і оригінала секретного графічного повідомлення (зображення « X ») на рис. 7.

Зауважимо, що для роботи запропонованого алгоритму можна використовувати й інші вейвлет-перетворення (Морле, Хаара тощо). Також у якості контейнера можна застосовувати кольорові зображення RGB чи CMY, що дає змогу поглиблювати рівень шифрування або збільшувати розмір секретного графічного повідомлення, яке підлягає передачі.

Слід також зауважити те, що переданим може бути не зображення, а матриця коефіцієнтів. Це також утруднює атаку стегано-файлу – на якому носієві-зображенні йде повідомлення. Вибір носія-зображення може бути оголошеним в останню мить. Безперечно, що при дефіциті часу, особливо коли цінність конфіденційного повідомлення з часом стає нульовою, дешифрування повідомлення буде досить проблематичним.

6. Перспективи подальших досліджень. Автори вважають перспективними напрямки досліджень, пов'язані зі створенням стегоконтейнерів, що містять приховану графічну інформацію на основі рухомих зображень, що є відео-файлами (неперервний потік кодованої інформації), та вейвлетів. Також важливим є дослідження алгоритмів такого типу за обчислювальною складністю, пропускною здатністю каналу та стеганостійкістю [3].

Список літератури: 1. *Задірака В.К., Мельникова С.С., Бородавка Н.В.* Спектральні алгоритми комп'ютерної стеганографії //Искусственный интеллект. - 2002. - № 3.- С.532 - 541. **2.** *Бородавка Н.В., Задирака В.К.* Стеганоалгоритмы на базе теоремы о свертке // Кибернетика и системный анализ.-2004.-№1.-С. 139- 144. **3.** *Задірака В.К., Мельникова С.С., Кошкіна Н.В.* Ефективні алгоритми побудови стегоконтейнерів з використанням швидкого перетворення Фур'є. Праці Міжнародної конференції «Питання оптимізації обчислень (ПОО XXXII)», присвяченої пам'яті академіка В.С. Михалевича. – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України, 2005. – С. 78-79. **4.** *Ященко В. В.* Введение в криптографию. – М.: МЦНМО – ЧеРо, 1999. – 186 с. **5.** *Шмаев В. Б.* Современная стеганография. Принципы, основные носители и методы противодействия. http://www.re.mipt.ru/infsec **6.** *Дороботя А. І., Манжула О. В., Кулик С. І.* Шифрування зображень з використанням алгоритму RSA та вейвлетів Добеші. Збірник наукових праць Бердянського державного педагогічного університету (Педагогічні науки). – № 3. – Бердянськ: БДПУ, 2005. – С. 189-197. **7.** *Добеши И.* Десять лекций по вейвлетам. – М.: Ижевск: НИЦ „Регулярная и хаотическая динамика", 2001. - 464 с.

Надійшла до редколегії 06.10.2010