УДК 519.6

А. І. Дроботя*, канд. техн. наук,
С. І. Кулик,** канд. фіз.-мат. наук,
О. О. Литвин*,** канд. фіз.-мат. наук,
*Бердянський державний педагогічний університет, м. Бердянськ,
**Національний технічний університет «ХПІ», м. Харків,
***Українська інженерно-педагогічна академія, м. Харків

СТВОРЕННЯ СТЕГОФАЙЛУ НА ЗОБРАЖЕННІ-КОНТЕЙНЕРІ З ВИКОРИСТАННЯМ ВЕЙВЛЕТІВ

У статті запропоновано метод створення стегоповідомлення на основі статичного зображення та вейвлетів. На конкретному прикладі (передача секретного текстового повідомлення) розглянуто роботу розробленого алгоритму, наведено результати роботи програми (в якості прикладу використано вейвлети Добеші четвертого порядку) та наведено аналіз результатів проведеного обчислювального експерименту. Також розглянуто перспективи подальших досліджень.

Ключові слова: *стеганологія, стеганографія, криптографія, криптоалгоритм, стегоконтейнер, вейвлети, вейвлет-перетворення.*

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.

Аналіз останніх досліджень. Незначна змінюваність первинних образів після “вживлення” стегоповідомлення, що не провокує підозр щодо наявності в них сторонньої інформації описана 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 тексту в інформацію зображення-контейнера та вилучення його звідти.

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 як функції двох змінних $f(x, y)$ та «приклеюванні» кодів символів прихованого повідомлення до мантиси обраного вейвлет-коефіцієнта і подальшому застосуванні оберненого вейвлет-перетворення до матриці «спотворених» вейвлет-коефіцієнтів.

Задача дешифрування полягає у вилученні кодів символів зашифрованого повідомлення шляхом застосування прямого вейвлет-перетворення отриманої матриці «спотвореного» зображення та порівняння з матрицею вейвлет-перетворення використовуваного зображення. Слід підкреслити, що вибір послідовності коефіцієнтів матриці вейвлет-перетворення для «приклеювання» надає досить широкі можливості додаткового ускладнення ситуації проти спроб атаки стегоповідомлення. Залишаємо поза обговоренням те, що сам текст може бути оброблено якимось криптографічним алгоритмом [6].

Основні результати. Перейдемо до особи, яка передає повідомлення. Отже, будемо розглядати підготовче перетворення 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 стегофайл. 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 СКМ MathCad зводиться до роботи з матрицею $A.$ На рис. 1 бачимо еталонне зображення «Lena» (512×512 пікселів) та матрицю $L,$ 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 $f(x, y)$. Отримаємо

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

L

L =

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	135	140	129	115	116	120	112	124	113	109	123	120	119
1	133	140	148	126	114	120	120	136	122	116	118	116	106
2	135	135	150	152	124	111	124	130	129	111	109	102	92
3	152	134	134	160	137	113	124	127	123	113	113	107	93
4	157	137	120	138	151	127	125	126	114	106	101	102	104
5	153	154	122	134	147	145	129	122	104	93	95	113	112
6	137	161	146	139	133	143	132	119	98	94	102	113	117
7	130	157	164	161	130	123	127	113	94	109	118	113	115
8	136	132	153	166	142	116	109	97	90	110	118	120	119
9	153	122	133	143	153	116	107	106	99	106	118	116	128
10	163	132	121	134	144	122	105	111	107	114	116	123	134
11	168	151	119	126	120	107	102	113	117	112	113	124	136
12	167	167	132	116	100	95	105	113	122	123	125	130	136
13	151	171	148	104	93	103	108	122	126	133	131	136	142
14	136	155	156	110	95	102	117	129	127	125	130	136	140
15	131	131	127	103	98	102	111	133	126	122	121	125	133
16	128	105	98	89	97	116	125	134	130	125	120	119	125
17	154	108	89	88	103	127	140	128	132	134	132	121	122
18	161	116	95	98	105	136	143	127	130	139	132	123	124
19	143	107	100	109	123	140	137	132	129	129	136	129	127
20	147	116	103	128	130	134	133	130	127	127	131	133	124

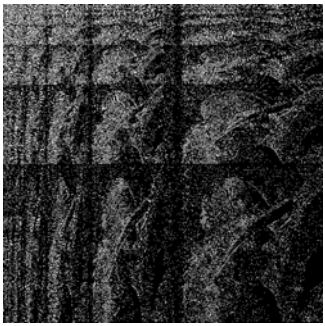
Рис. 1. *Еталонне зображення «Lena» та матриця, що йому відповідає*

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. Підготовлений певний текст T, який підлягає передачі в умовах конфіденційності може містити кількість символів не більшу, ніж кількість коефіцієнтів матриці. Він може бути, безумовно, попередньо закодований якимось з криптоалгоритмів.

PP =

	0	1	2
0	4606.96409179229	7704.41621696637	487.032456607334
1	6050.22452438171	7480.6451668596	-697.659893838999
2	916.926423928195	-1450.48767909914	1105.003115625
3	-610.812345629038	81.9915810500553	63.1124743103356
4	588.321190840651	-602.373919853406	269.540647866783
5	-282.215811723736	161.722655804639	70.6591513687862
6	-9.59681211914638	-503.113104653493	99.5902500529092
7	-15.6702165779514	415.959081549769	-375.519475874969
8	400.946272095993	-234.908451674457	120.345106939552
9	-22.174544962814	-23.0608405464872	59.4681990454767
10	-45.210795785316	-46.1799469412108	95.8790482029225
11	-79.8652946118909	117.552291983572	-94.601078975772
12	-85.6285872404423	288.428909518901	-66.7581778584518
13	-84.350381442331	-219.824395473583	22.3179101835777
14	19.240527641786	153.253432753128	-26.8846840139546
15	-39.1916454111085	-34.7978218978546	-290.7356841079



$\frac{PP}{7}$

Рис. 2. *Матриця отриманих вейвлет-коефіцієнтів Добеші та відповідне їй зображення*

Обробка текстового повідомлення, на другому етапі, полягає у створенні послідовності ASCII-кодів, які відповідають символам. Довжина кожного коду, як відомо, обмежується трьома цифрами. На цьому етапові отримуємо функцію $ASCII(T)$, що містить коди символів прихованого повідомлення. На рис. 3 зображено вектор-рядок кодів *ASCII* символів повідомлення: «Nastupnyi Etap–Peredacha grafichnyh povidomlen' u Stego Conteyneri».

V =

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	78	97	115	116	117	112	110	121	105	32	69	116	97	112	45	80	1

Рис. 3. *Частина отриманого вектор-рядка отриманих кодів символів прихованого повідомлення*

3. На третьому етапові виконуємо «приклеювання» кодів (в числовій формі) до коефіцієнтів Добеші. 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» кодів символів $ASCII(T)$ прихованого повідомлення T до коефіцієнтів Добеші. Можливості варіювати «приклеювання» досить широкі: можна розміщувати за елементами діагоналі, за рядками чи стовпчиками, випадковим чином, за домовленим порядком тощо. Функція d може бути, наприклад, функцією, що залежить від часу. В результаті отримаємо:

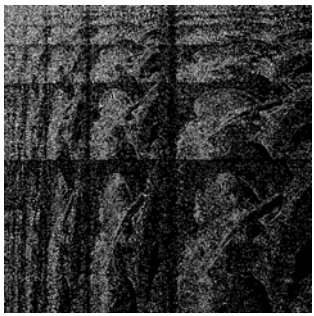
$$g(x,y) = f'(x,y) + S(x,y), \tag{1}$$

де $S(x,y) = d\left[ASCII(T) \right]$.

В нашому прикладі додамо числові коди символів прихованого повідомлення до діагональних елементів матриці коефіцієнтів вейвлет-перетворення (рис. 4).

PPzminen =

	0	1	2
0	4606.96409	7704.41621	487.032456
1	6050.22452	7480.6451	-697.659893
2	916.926423	-1450.48767	1105.00
3	-610.812345	81.9915810	63.1124743
4	588.321190	-602.373919	269.540647
5	-282.215811	161.722655	70.6591513
6	-9.59681211	-503.113104	99.5902500
7	-15.6702165	415.959081	-375.519475
8	400.946272	-234.908451	120.345106
9	-22.174544	-23.0608405	59.4681990
10	-45.210795	-46.1799469	95.8790482
11	-79.8652946	117.552291	-94.601078
12	-85.6285872	288.428909	-66.7581778
13	-84.350381	-219.824395	22.3179101
14	19.240527	153.253432	-26.8846840
15	-39.1916454	-34.7978218	-290.7356



$\frac{PPzminen}{7}$

Рис. 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 $g(x,y)$.

$$\overline{g}(x,y) = IWg(x,y) \text{ або } g(x,y) \xrightarrow{IW} \overline{g}(x,y).$$

На рис. 5 наведено еталонне зображення L і «спотворене» зображення Q. Залишається передати «спотворене» зображення Q з повідомленням адресатові.

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 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

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

L Q

Рис. 5. *Візуальне порівняння еталонного зображення L і «спотвореного» зображення Q*

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 текстове повідомлення T здійснивши зворотні дії:

$$ASCII(T) = d^{-1}\left[S(x,y)\right],$$

$$T = \left[ASCII(T)\right]^{-1}.$$

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

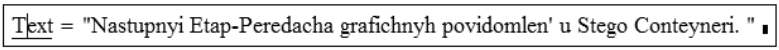


Рис. 6. *Результат роботи програми з вилучення прихованого повідомлення із отриманого файлу*

Висновки. У роботі реалізовано алгоритм створення стегофайлу на стандартному зображенні-контейнері — «Lena», що представлене у «градаціях сірого» з використанням вейвлетів Добеші 4-го порядку. Про це свідчить візуальне порівняння еталонного зображення L і зображення Q отриманого стегофайлу — рис. 5, а також результат роботи програми дешифрування, показаний на рис. 6.

Зауважимо, що для роботи запропонованого алгоритму можна використовувати й інші вейвлет-перетворення (Морле, Гаара тощо).

Також у якості контейнера можна застосовувати кольорові зображення RGB чи CMY, що дає змогу поглиблювати рівень шифрування або збільшувати розмір 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.

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

Список використаних джерел:

1. Задірака В. К. Спектральні алгоритми комп'ютерної стеганографії / В. К. Задірака, С. С. Мельникова, Н. В. Бородавка // Искусственный интеллект. — 2002. — № 3. — С. 532—541.

2. Бородавка Н. В. Стеганоалгоритмы на базе теоремы о свертке / Н. В. Бородавка, В. К. Задирака // Кибернетика и системный анализ. — 2004. — №1. — С. 139–144.
3. Задірака В. К. Ефективні алгоритми побудови стегоконтейнерів з використанням швидкого перетворення Фур'є / В. К. Задірака, С. С. Мельникова, Н. В. Кошкіна. — К. : Інститут кібернетики ім. В. М. Глушкова НАН України, 2005. — С. 78–79.
4. Ященко В. В. Введение в криптографию / В. В. Ященко. — М. : МЦНМО-ЧеРо, 1999. — 186 с.
5. Шмаев В. Б. Современная стеганография. Принципы, основные носители и методы противодействия / В. Б. Шмаев. — Режим доступу: http://www.re.mipt.ru/infsec
6. Дороботя А. І. Шифрування зображень з використанням алгоритму RSA та вейвлетів Добеші / А. І. Дороботя, О. В. Манжула, С. І. Кулик // Збірник наукових праць Бердянського державного педагогічного університету (Педагогічні науки). — № 3. — Бердянськ : БДПУ, 2005. — С. 189–197.
7. Добеши И. Десять лекций по вейвлетам / И. Добеши. — М. ; Ижевск : НИЦ «Регулярная и хаотическая динамика», 2001. — 464 с.

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

Key words: *steganology, steganolography, cryptography, cryptoalgorithm, stegocontainer, wavelet, wavelet transform.*

Отримано 31.09.10