УДК 004.056 (045)
DOI: 10.18372/2310-5461.34.11610

О. К. Юдін — д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-5098-7796
e-mail: yak333@ukr.net;

Я.А. Симониченко — аспірант
Національний авіаційний університет
orcid.org/0000-0002-9404-6610
e-mail: yaroslavsim@ukr.net;

А. А. Симониченко
Національний авіаційний університет
orcid.org/0000-0001-5317-3464
e-mail: annasim98@ukr.net;

ДОСЛІДЖЕННЯ СУЧАСНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ТА ЗАСОБІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ

Вступ

Постійне згадування в засобах масової інформації технології приховування повідомлення в інформаційних об'єктах (графічних файлах, відеофайлах, аудіофайлах та ін.) — підвищило зацікавленість суспільства до зазначеної технології та можливості її використання з метою забезпечення конфіденційності інформації. Однією із сучасних технологій, яка використовується для вирішення даного питання є стеганографічний захист інформації.

Велика кількість сучасних програмних стеганографічних засобів зробили вищезазначену технологію доступною для будь-якого пересічного громадянина, що може використовувати її для реалізації різних поставлених цілей. Ще у вересні 2001 р., ЗМІ опублікували інформацію про те, що «Аль-Каїда», під час підготовці теракту та атаки на Всесвітній торговий центр в США, користувалася методами стеганографії для передачі повідомлень.

Як наслідок, реалізація вищезазначених технологій приховування інформації може використовуватися з метою організації захисту інформації або з метою організації прихованого каналу передачі (витоку) інформації.

Постановка завдання

Сукупність засобів і методів, що використовуються для формування прихованого каналу передачі інформації утворюють стеганографічну систему [1, с. 71]. Дана система виконує вбудовування повідомлення (прихованої інформації) в інформаційний об'єкт (далі — ІО) одним із стеганографічних методів. Передавання ІО каналами зв'язку та виділення приховуваного повідомлення з отриманого ІО. Найбільш уніфікованим ІО, що використовується стеганографічними засобами є графічний файл, а прихованою інформацією є текстове повідомлення [2, с. 390]. Однією з основних характеристик стеганографічної системи, при створенні прихованого каналу передачі інформації, є його пропускна спроможність. Під пропускною спроможністю каналу передачі прихованої інформації розуміється максимальна кількість інформації, що може бути вбудована в один елемент ІО (наприклад, піксель зображення або його колірної компоненти при використанні моделі RGB) з використанням стеганографічних методів.

За принципом приховування, стеганографічні методи поділяють на два основні класи:

– безпосередньої заміни (використовують надлишковість ІО в просторовій (для зображення) або часовій (для звуку) області та полягають у заміні малозначущих частин контейнера елементами (бітами) прихованого повідомлення);

– спектральні методи (використовують спектральне представлення елементів ІО, у яке виконується вбудовування елементів прихованого повідомлення).

Найчастіше, як стеганографічні засоби виступають стеганографічні програмні продукти.

Таким чином, **метою даної статті** є дослідження сучасних стеганографічних методів та засобів обробки цифрових зображень з використанням програмних засобів, що вільно розповсюджуються через мережу Інтернет.

Під час дослідження буде виконано виявлення структурних змін у графічних файлах-результатах, що будуть отримані при використанні сучасних стеганографічних програмних засобів, в порівнянні з файлом-оригіналом, а також, зображення-результатів та зображення-оригіналу. На основі проведених досліджень будуть отримані

результати, щодо сучасних методів реалізації приховування інформації стеганографічними програмними засобами, які буде можливо використовувати при подальшому для підвищення ефективності стеганографічної системи або стеганографічного аналізу.

Одним з головних завдань стеганографічного аналізу є дослідження можливих слідів застосування стеганографічних засобів та розробка методів, що дозволяють виявляти факти їх використання.

Як метод дослідження, буде реалізований один із методів стеганографічного аналізу, а саме — атака на основі відомого порожнього ІО, що дає можливість шляхом порівняння його із заповненим ІО встановити факт наявності прихованої інформації. Таким чином, у рамках даного дослідження будуть виконані такі порівняння файлу/зображення — результату та файлу/зображення — оригіналу:

– зміна розміру графічного файлу-результату порівняно із файлом-оригіналом;

– підрахунок кількості модифікованих значень пікселів зображення-результату та зображення-оригіналу;

– дослідження модифікації колірних компонентів зображення-оригіналу та їх відповідних бітових площин;

– порівняння структури отриманих графічних файлів-результатів із файлом-оригіналом.

Розв’язання проблеми

Для дослідження стеганографічних методів було використано більше 20 програмних засобів (продуктів) приховування інформації (далі — ПЗ), які доступні пересічному громадянину та вільно розповсюджуються через мережу Інтернет, а саме:

- Camouflage (далі — ПЗ1);
- Clotho (далі — ПЗ2);
- DeEgger Embedder (далі — ПЗ3);
- FIRA2 (далі — ПЗ4);
- HexaStego—BMP (далі — ПЗ5);
- Hide&Reveal (далі — ПЗ6);
- ImageSpyer (далі — ПЗ7);
- ImageSpyer G2 (далі — ПЗ8);
- JHide (далі — ПЗ9);
- Our Secret (далі — ПЗ10);
- QuickStego (далі — ПЗ11);
- Shusssh! (далі — ПЗ12);
- SilentEye (далі — ПЗ13);
- Steganos Privacy Suite 18 (далі — ПЗ14);
- Steganos Security Suite 2007 (далі — ПЗ15);
- SteganoG (далі — ПЗ16);
- SteganographX Plus (далі — ПЗ17);
- S-Tools (далі — ПЗ18);
- Xiao Steganography (далі — ПЗ19);
- Anubis (далі — ПЗ20);
- Hallucinate (далі — ПЗ21);
- OpenPuff (далі — ПЗ22).

Як ІО використовувався графічний файл BMP-формату, оскільки він є оптимальнішим форматом при виконанні стеганоперетворення [3, с.77]. Розмір зображення — 635×500 пікселів, а глибина кольору — 24 біти (рис. 1).

Рис. 1. Зображення для приховування повідомлення

Припустимо, що вбудовування прихованого повідомлення в обране зображення буде виконуватися «класичним» методом безпосередньої заміни молодшого біту в компоненті синього кольору при використанні колірної моделі RGB. Для кодування градацій кольору кожної компоненти моделі RGB використовується 8 біт (загалом 24 біти для кодування 3-х кольорів компонент). Загальна кількість молодших бітів у даній компоненті становить — 317500. Як приховане повідомлення було обрано три текстових повідомлення англійською мовою довжиною — 1983 символів (15864 біт), 5 946 символів (47568 біт) та 9910 символів (79280 біт), що відповідно становить 5, 15 та 25 % від загальної кількості пікселів колірної компоненти зображення та відповідає пропускній спроможності каналу зв’язку. Збереження повідомлення відбувалося в текстовий файл із TXT-форматом.

При використанні вищезазначених ПЗ, також існує можливість контролю цілісності прихованого повідомлення (Xiao Steganography), використання попереднього криптографічного захисту повідомлення (Clotho, SilentEye та ін.) та захисту повідомлення від несанкціонованого ознайомлення з використанням паролю (Camouflage, FIRA2 та ін.). Більшу частину досліджуваних ПЗ виконують зазначені дії за замовчуванням, але в рамках даного дослідження будемо розглядати лише механізм приховування повідомлення.

Виконаємо дослідження зміни показника розміру графічного файлу-результату порівняно із файлом-оригіналом, що має розмір — 952054 байти (рис. 2). Оскільки, протягом дослідження обрано три повідомлення різного розміру, було отримано три відповідних графічних файлів-результатів для кожного ПЗ із прихованими повідомленнями. Наприклад, використовуючи ПЗ1 (програмний продукт — Camouflage), було

отримано: три графічні файли, а саме: графічний файл із 5 % прихованим повідомленням (далі — ПЗ1/1), графічний файл із 15 % прихованим повідомленням (далі — ПЗ1/2) та графічний файл із 25 % прихованим повідомленням (далі — ПЗ1/3).

Таким чином, позначення відповідних графічних файлів-результатів, має такий вигляд: ПЗ*x*/1 (заповнення — 5 %), ПЗ*x*/2 (заповнення — 15 %) та ПЗ*x*/3 (заповнення — 25 %), де *x* — позначення відповідного програмного продукту.

З рис. 2 можна побачити, показник розміру файлів-результатів для ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12, ПЗ19 та ПЗ20 суттєво відрізняється від розміру файлу-оригіналу та прямо пропорційно збільшується з розміром прихованого повідомлення. Розміри файлів-результатів інших ПЗ, після приховування повідомлення, відповідають розміру файлу-оригіналу.

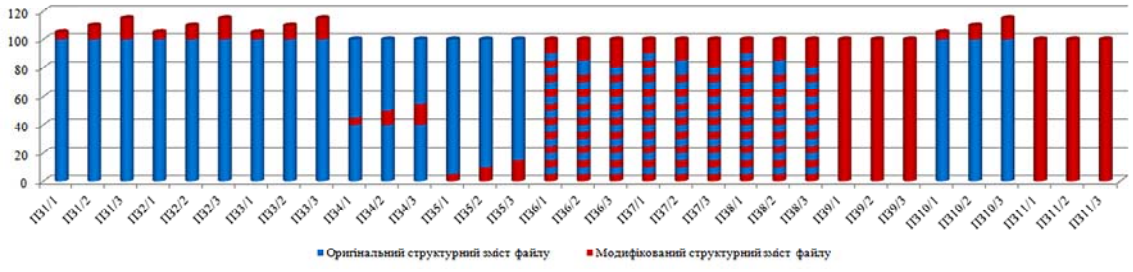
Виконаємо порівняння структури отриманих графічних файлів-результатів із файлом-оригіналом (рис. 3). Порівняння структурного змісту та розмірів графічних файлів-результатів, при використанні ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12, ПЗ19 та ПЗ20, дає можливість попередньо зробити висновок відносно методу приховування повідомлення даними ПЗ.

Таким чином, з огляду на вищезазначене, дані ПЗ виконують звичайне додавання прихованого повідомлення в кінець графічного файлу з використанням методу «склеювання».

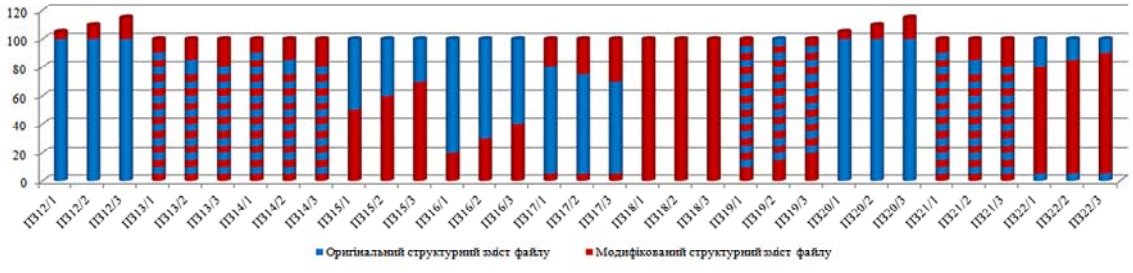
а

б

Рис. 2. Графічне відображення показника розмірів файлів-результатів: *а* — ПЗ1-11; *б* — ПЗ12-22



а



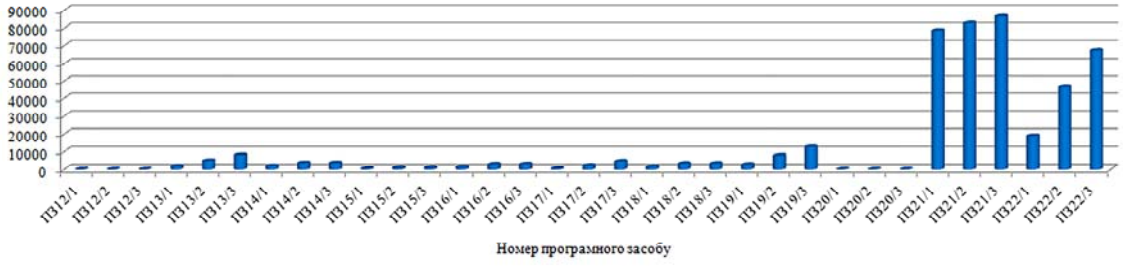
б

Рис. 3. Графічне відображення порівняння структури файлів-результатів: *а* — ПЗ1-11; *б* — ПЗ12-22

Порівняння файлів-результатів інших ПЗ, свідчить про використання стеганографічних методів приховування інформації, що призвели до зміни структурного змісту файлу порівняно із файлом-оригіналом та збереження розміру файлів після стеганоперетворення.

Виконаємо більш детальніше дослідження зображень-результатів, а саме: кількості модифікованих значень пікселів зображень-результатів із зображенням-оригіналом (рис. 4) та модифікації їх колірних компонентів (табл. 1). Як можна побачити з рис. 4, зображення-результат, утворені ПЗ4, ПЗ5, ПЗ6, ПЗ7, ПЗ8, ПЗ9, ПЗ11, ПЗ13, ПЗ14, ПЗ15, ПЗ16, ПЗ17, ПЗ18, ПЗ19, ПЗ21 та ПЗ22, відрізняються від зображення-оригіналу. У більшості випадків, кількість модифікованих значень пікселів зображення залежить від розміру прихованого повідомлення: чим більший розмір повідомлення — тим більша кількість модифікованих пікселів. Зображення-результат, утворені ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12 та ПЗ20, залишились без змін, оскільки приховування повідомлення в даних ПЗ виконується методом «склеювання».

а



б

Рис. 4. Кількість модифікованих значень пікселів зображень-результатів; *а* — ПЗ1-11; *б* — ПЗ12-22

Таблиця 1

Дослідження модифікації колірних компонентів зображення-результату

№	ПЗ	R	G	B	№	ПЗ	R	G	B
1.	**ПЗ1/1**	–	–	–	34.	**ПЗ12/1**	–	–	–
2.	**ПЗ1/2**	–	–	–	35.	**ПЗ12/2**	–	–	–
3.	**ПЗ1/3**	–	–	–	36.	**ПЗ12/3**	–	–	–
4.	**ПЗ2/1**	–	–	–	37.	**ПЗ13/1**	+	+	+
5.	**ПЗ2/2**	–	–	–	38.	**ПЗ13/2**	+	+	+
6.	**ПЗ2/3**	–	–	–	39.	**ПЗ13/3**	+	+	+
7.	**ПЗ3/1**	–	–	–	40.	**ПЗ14/1**	+	+	+
8.	**ПЗ3/2**	–	–	–	41.	**ПЗ14/2**	+	+	+
9.	**ПЗ3/3**	–	–	–	42.	**ПЗ14/3**	+	+	+
10.	**ПЗ4/1**	+	+	+	43.	**ПЗ15/1**	+	+	+
11.	**ПЗ4/2**	+	+	+	44.	**ПЗ15/2**	+	+	+
12.	**ПЗ4/3**	+	+	+	45.	**ПЗ15/3**	+	+	+
13.	**ПЗ5/1**	+	+	+	46.	**ПЗ16/1**	+	+	+
14.	**ПЗ5/2**	+	+	+	47.	**ПЗ16/2**	+	+	+
15.	**ПЗ5/3**	+	+	+	48.	**ПЗ16/3**	+	+	+
16.	**ПЗ6/1**	+	+	+	49.	**ПЗ17/1**	+	–	–
17.	**ПЗ6/2**	+	+	+	50.	**ПЗ17/2**	+	–	–
18.	**ПЗ6/3**	+	+	+	51.	**ПЗ17/3**	+	–	–
19.	**ПЗ7/1**	+	+	+	52.	**ПЗ18/1**	+	+	+

№	ПЗ	R	G	B	№	ПЗ	R	G	B
20.	**ПЗ7/2**	+	+	+	53.	**ПЗ18/2**	+	+	+
21.	**ПЗ7/3**	+	+	+	54.	**ПЗ18/3**	+	+	+
22.	**ПЗ8/1**	+	+	+	55.	**ПЗ19/1**	+	+	+
23.	**ПЗ8/2**	+	+	+	56.	**ПЗ19/2**	+	+	+
24.	**ПЗ8/3**	+	+	+	57.	**ПЗ19/3**	+	+	+
25.	**ПЗ9/1**	+	+	+	58.	**ПЗ20/1**	–	–	–
26.	**ПЗ9/2**	+	+	+	59.	**ПЗ20/2**	–	–	–
27.	**ПЗ9/3**	+	+	+	60.	**ПЗ20/3**	–	–	–
28.	**ПЗ10/1**	–	–	–	61.	**ПЗ21/1**	+	+	+
29.	**ПЗ10/2**	–	–	–	62.	**ПЗ21/2**	+	+	+
30.	**ПЗ10/3**	–	–	–	63.	**ПЗ21/3**	+	+	+
31.	**ПЗ11/1**	+	+	+	64.	**ПЗ22/1**	+	+	+
32.	**ПЗ11/2**	+	+	+	65.	**ПЗ22/2**	+	+	+
33.	**ПЗ11/3**	+	+	+	66.	**ПЗ22/3**	+	+	+

При використанні 24-х бітового зображення, для кодування кожної колірної компоненти зображення моделі RGB, де R — червоний (Red), G — зелений (GREEN), B — синій (Blue), використовується по 8 біт. Кожна колірна компонента складається з восьми бітових площин відповідної розрядності (0…8). При використанні вищезазначених ПЗ, модифікація всіх 3-х колірних компонентів виконується — ПЗ4, ПЗ5, ПЗ6, ПЗ7, ПЗ8, ПЗ9, ПЗ11, ПЗ13, ПЗ14, ПЗ15, ПЗ16, ПЗ18, ПЗ19, ПЗ21 та ПЗ22, а модифікація однієї, червоної колірної компоненти, виконалась — ПЗ17.

При більш детальнішому дослідженні зображень-результатів, можна побачити, що модифікація бітових площин колірних компонентів відбулася при використанні ПЗ4, ПЗ5, ПЗ6, ПЗ7, ПЗ8, ПЗ9, ПЗ11, ПЗ13, ПЗ14, ПЗ15, ПЗ16, ПЗ17, ПЗ18, ПЗ19, ПЗ21, ПЗ22 (відповідно до табл. 2).

Таблиця 2

Дослідження модифікації бітових площин колірних компонентів зображення-результату

№	ПЗ	Номер бітової площини											
		Red				Green				Blue			
		0	1	2	3	0	1	2	3	0	1	2	3
1.	**ПЗ1/1**	–	–	–	–	–	–	–	–	–	–	–	–
2.	**ПЗ1/2**	–	–	–	–	–	–	–	–	–	–	–	–
3.	**ПЗ1/3**	–	–	–	–	–	–	–	–	–	–	–	–
4.	**ПЗ2/1**	–	–	–	–	–	–	–	–	–	–	–	–
5.	**ПЗ2/2**	–	–	–	–	–	–	–	–	–	–	–	–
6.	**ПЗ2/3**	–	–	–	–	–	–	–	–	–	–	–	–
7.	**ПЗ3/1**	–	–	–	–	–	–	–	–	–	–	–	–
8.	**ПЗ3/2**	–	–	–	–	–	–	–	–	–	–	–	–
9.	**ПЗ3/3**	–	–	–	–	–	–	–	–	–	–	–	–
10.	**ПЗ4/1**	+	+	–	–	+	+	–	–	+	+	–	–
11.	**ПЗ4/2**	+	+	–	–	+	+	–	–	+	+	–	–
12.	**ПЗ4/3**	+	+	–	–	+	+	–	–	+	+	–	–
13.	**ПЗ5/1**	+	+	–	–	+	+	–	–	+	+	–	–
14.	**ПЗ5/2**	+	+	–	–	+	+	–	–	+	+	–	–
15.	**ПЗ5/3**	+	+	–	–	+	+	–	–	+	+	–	–
16.	**ПЗ6/1**	+	–	–	–	+	–	–	–	+	–	–	–
17.	**ПЗ6/2**	+	–	–	–	+	–	–	–	+	–	–	–
18.	**ПЗ6/3**	+	–	–	–	+	–	–	–	+	–	–	–
19.	**ПЗ7/1**	+	+	+	–	+	+	+	–	+	+	–	–
20.	**ПЗ7/2**	+	+	+	–	+	+	+	–	+	+	–	–
21.	**ПЗ7/3**	+	+	+	–	+	+	+	–	+	+	–	–
22.	**ПЗ8/1**	+	+	+	–	+	+	+	–	+	+	–	–
23.	**ПЗ8/2**	+	+	+	–	+	+	+	–	+	+	–	–

№	ПЗ	Номер бітової площини											
		Red				Green				Blue			
		0	1	2	3	0	1	2	3	0	1	2	3
24.	**ПЗ8/3**	+	+	+	–	+	+	+	–	+	+	–	–
25.	**ПЗ9/1**	+	+	–	–	+	+	–	–	+	+	–	–
26.	**ПЗ9/2**	+	+	–	–	+	+	–	–	+	+	–	–
27.	**ПЗ9/3**	+	+	–	–	+	+	–	–	+	+	–	–
28.	**ПЗ10/1**	–	–	–	–	–	–	–	–	–	–	–	–
29.	**ПЗ10/2**	–	–	–	–	–	–	–	–	–	–	–	–
30.	**ПЗ10/3**	–	–	–	–	–	–	–	–	–	–	–	–
31.	**ПЗ11/1**	+	–	–	–	+	–	–	–	+	–	–	–
32.	**ПЗ11/2**	+	–	–	–	+	–	–	–	+	–	–	–
33.	**ПЗ11/3**	+	–	–	–	+	–	–	–	+	–	–	–
34.	**ПЗ12/1**	–	–	–	–	–	–	–	–	–	–	–	–
35.	**ПЗ12/2**	–	–	–	–	–	–	–	–	–	–	–	–
36.	**ПЗ12/3**	–	–	–	–	–	–	–	–	–	–	–	–
37.	**ПЗ13/1**	+	+	+	–	+	+	+	–	+	+	+	–
38.	**ПЗ13/2**	+	+	+	–	+	+	+	–	+	+	+	–
39.	**ПЗ13/3**	+	+	+	–	+	+	+	–	+	+	+	–
40.	**ПЗ14/1**	+	–	–	–	+	–	–	–	+	–	–	–
41.	**ПЗ14/2**	+	–	–	–	+	–	–	–	+	–	–	–
42.	**ПЗ14/3**	+	–	–	–	+	–	–	–	+	–	–	–
43.	**ПЗ15/1**	+	–	–	–	+	–	–	–	+	–	–	–
44.	**ПЗ15/2**	+	–	–	–	+	–	–	–	+	–	–	–
45.	**ПЗ15/3**	+	–	–	–	+	–	–	–	+	–	–	–
46.	**ПЗ16/1**	+	+	–	–	+	+	–	–	+	+	–	–
47.	**ПЗ16/2**	+	+	–	–	+	+	–	–	+	+	–	–
48.	**ПЗ16/3**	+	+	–	–	+	+	–	–	+	+	–	–
49.	**ПЗ17/1**	+	–	–	–	–	–	–	–	–	–	–	–
50.	**ПЗ17/2**	+	–	–	–	–	–	–	–	–	–	–	–
51.	**ПЗ17/3**	+	–	–	–	–	–	–	–	–	–	–	–
52.	**ПЗ18/1**	+	–	–	–	+	–	–	–	+	–	–	–
53.	**ПЗ18/2**	+	–	–	–	+	–	–	–	+	–	–	–
54.	**ПЗ18/3**	+	–	–	–	+	–	–	–	+	–	–	–
55.	**ПЗ19/1**	+	–	–	–	+	–	–	–	+	–	–	–
56.	**ПЗ19/2**	+	–	–	–	+	–	–	–	+	–	–	–
57.	**ПЗ19/3**	+	–	–	–	+	–	–	–	+	–	–	–
58.	**ПЗ20/1**	–	–	–	–	–	–	–	–	–	–	–	–
59.	**ПЗ20/2**	–	–	–	–	–	–	–	–	–	–	–	–
60.	**ПЗ20/3**	–	–	–	–	–	–	–	–	–	–	–	–
61.	**ПЗ21/1**	+	+	+	+	+	+	+	+	+	+	+	+
62.	**ПЗ21/2**	+	+	+	+	+	+	+	+	+	+	+	+
63.	**ПЗ21/3**	+	+	+	+	+	+	+	+	+	+	+	+
64.	**ПЗ22/1**	+	–	–	–	+	–	–	–	+	–	–	–
65.	**ПЗ22/2**	+	–	–	–	+	–	–	–	+	–	–	–
66.	**ПЗ22/3**	+	–	–	–	+	–	–	–	+	–	–	–

Таким чином, під час дослідження, було використано більше 20 програмних засобів (продуктів) приховування інформації (далі — ПЗ), які доступні пересічному громадянину. Було виконано порівняння структури графічних файлів-результатів із файлом-оригіналом, а також, зображення-результатів та зображення-оригіналу.

Ураховуючи показник зміни розміру графічного файлу-результату та порівняння структури отриманих графічних файлів-результатів, можна зробити висновок, що використання 6 програмних засобів призводить до збільшення розміру отриманого файлу, оскільки вони виконують додавання прихованого повідомлення в кінець гра-

фічного файлу з використанням методу «склеювання». До таких програмних засобів приховування повідомлення відносяться — ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12 та ПЗ20.

Приховування повідомлення іншими програмними засобами виконується з використанням стеганографічних методів безпосередньої заміни малозначущих частин зображення (надлишкової інформації) бітами прихованого повідомлення. З огляду на результати показника порівняння структури, можливо зробити попередній висновок відносно стеганографічних методів, що використовуються: ПЗ4, ПЗ5, ПЗ9, ПЗ11, ПЗ15, ПЗ16, ПЗ17, ПЗ18 та ПЗ22 — виконують послідовну заміну надлишкової інформації бітами прихованого повідомлення, а ПЗ7, ПЗ8, ПЗ13, ПЗ14, ПЗ19 та ПЗ21 — виконують приховування та розподіл бітів прихованого повідомлення у файлі з певним інтервалом.

При дослідженні колірних компонентів зображення-оригіналу та їх відповідних бітових площин, можна визначити модифіковані бітові площини колірних компонентів зображення. У загальному випадку, під час дослідження, виконувалась модифікація лише чотирьох бітових площин із розрядністю «0», «1», «2» та «3». При використанні ПЗ6, ПЗ11, ПЗ14, ПЗ15, ПЗ17, ПЗ18, ПЗ19 та ПЗ22 виконується модифікація однієї бітової площини зображення із розрядністю «0». Використання ПЗ4, ПЗ5, ПЗ9 та ПЗ16 призводить до модифікації двох бітових площин зображення («0» та «1»). При використанні ПЗ7, ПЗ8 та ПЗ13 виконується модифікація трьох бітових площин зображення («0», «1» та «2»). ПЗ21 виконує модифікацію чотирьох бітових площин зображення («0», «1», «2» та «3»).

Ураховуючи кількість модифікованих значень пікселів та модифікацію колірних компонентів зображень-результатів, можна побачити, що програмні засоби, які використовують стеганографічні методи приховування інформації, виконують приховування повідомлення за рахунок модифікації бітових площин колірних компонентів зображення.

Висновок

Було виконано дослідження сучасних стеганографічних методів та засобів обробки цифрових зображень з використанням вищезазначених програмних засобів, що вільно розповсюджуються через мережу Інтернет. Під час дослідження, були виявлені структурні зміни у графічних файлах-результатах, що були отримані при використанні сучасних стеганографічних програмних засобів, в порівнянні із файлом-оригіналом, а також, їх зображень. Були виконані такі порівняння файлу/зображення-результату та файлу/зображення-оригіналу: зміна розміру графічних файлів; підрахунок кількості модифікованих значень пікселів зображень; дослідження модифікації колірних компонентів зображень та їх відповідних бітових площин; порівняння структури отриманих графічних файлів.

На основі проведених досліджень були отримані результати, щодо сучасних методів реалізації приховування інформації. Таким чином, частина програмних засобів виконує приховування повідомлення методом «склеювання», а інша частина — використовує стеганографічні методи безпосередньої заміни малозначущих частин зображення (надлишкової інформації) бітами прихованого повідомлення. Дані результати можна використовувати в подальшому для підвищення ефективності стеганографічної системи або стеганографічного аналізу.

Перспективи подальших досліджень

У свою чергу, на сьогодні, проведене дослідження та необхідність виявлення прихованих каналів передачі інформації, спонукає на створення нових уніфікованих методів стеганоаналізу та підвищення їх ефективності з використанням отриманих результатів.

ЛІТЕРАТУРА

1. **Юдін О. К.** Удосконалення стеганографічних методів на базі аналізу колірних моделей зображення / О. К. Юдін, Я. А. Симониченко // Наукоємні технології. — 2012. — №1 (13). — С. 70–75.

2. **Юдін О. К.** Виявлення прихованих каналів передачі інформації на базі методів стеганоаналізу / О. К. Юдін, Я. А. Симониченко // Наукоємні технології. — 2016. — №4 (32). — С. 389–394.

3. **Конахович Г. Ф.** Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

Юдін О. К., Симониченко Я. А., Симониченко А. А.

ДОСЛІДЖЕННЯ СУЧАСНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ТА ЗАСОБІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ

Проведено дослідження сучасних стеганографічних методів та засобів обробки цифрових зображень з використанням програмних засобів, що вільно розповсюджуються через мережу Інтернет та доступні пересічному громадянину. Під час дослідження, було виконано виявлення структурних змін у графічних файлах-результатах, а також, зображення-результатів та зображення-оригіналу. Були виконані такі порівняння: зміна розміру графічних файлів; підрахунок кількості модифікованих значень пікселів зображень; дослідження модифікації колірних компонентів зображень та їх відповідних бітових площин; порівняння структури отриманих графічних файлів. На основі проведених досліджень були отримані результати, щодо сучасних методів реалізації приховування інформації стеганографічними програмними засобами, які можливо використовувати в подальшому для підвищення ефективності стеганографічної системи або стеганографічного аналізу.

Ключові слова: стеганографічна система; стеганографічний аналіз; стеганографічний метод; стеганографічні програмні засоби.

Юдин А. К., Симониченко Я. А., Симониченко А. А.

ИССЛЕДОВАНИЯ СОВРЕМЕННЫХ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ И СРЕДСТВ ОБРАБОТКИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

В статье проведено исследование современных стеганографических методов и средств обработки цифровых изображений с использованием программных средств, которые свободно распространяются через сеть Интернет и доступны рядовому гражданину. Во время исследования, было выполнено выявления структурных изменений в графических файлах-результатах, а также, изображениях-результатах и изображения-оригинала. Были выполнены такие сравнения: изменение размера графических файлов; подсчет количества модифицированных значений пикселей изображений; исследование модификации цветовых компонентов изображений и их соответствующих битовых плоскостей; сравнение структуры полученных графических файлов. На основе проведенных исследований были получены результаты, относительно современных методов реализации скрытия информации стеганографическими программными средствами, которые возможно использовать в дальнейшем для повышения эффективности стеганографической системы или стеганографического анализа.

Ключевые слова: стеганографическая система; стеганографический анализ; стеганографический метод; стеганографические программные средства.

Yudin A. K, Simonichenko Ya. A., Simonichenko A. A.

RESEARCHES OF MODERN STEGANOGRAPHIC METHODS AND TOOLS FOR DIGITAL IMAGE TREATMENTS

The article deals with the study of modern steganographic methods and tools for processing digital images using software tools that are freely available through the Internet and available to the ordinary citizen. During the study, was performed identify the structural changes in graphics files which are the results, as well as, the result's images and the original's images. Was performed such comparisons: changes the size of graphics files; counting the number of modified pixel values of the images; study of the modification of the color image components and their respective bit planes; comparison of the structure of the received files. On the basis of the conducted researches were the results of relatively modern implementation methods hide information by steganography software that can be used in the future to improve the efficiency of steganographic system or steganographic analysis.

Keywords: steganography; steganography analysis; steganography; steganography software tools.

Стаття надійшла до редакції 31.05.2017 р.
Прийнято до друку 05.06.2017 р.
Рецензент – д-р техн. наук, проф. Конахович Г. Ф.