ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 621.391

МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Навроцький Д.О.

Розглянуті методи комп'ютерної стеганографії з точки зору можливості їх класифікації.

Вступ. Постановка задачі

Захист інформації (ЗІ) від несанкціонованого доступу - одна з найдавніших проблем. Як відомо, ціль криптографії полягає в блокуванні несанкціонованого доступу до інформації шляхом шифрування змісту повідомлень. Ціль стеганографії - сховати сам факт існування секретного повідомлення. При цьому, обидва способи можуть бути об'єднані і використані для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів). Комп'ютерні технології додали новий імпульс розвитку й удосконалюванню стеганографії, з'явився новий напрямок в області захисту інформації - комп'ютерна стеганографія (КС).

Основні принципи комп'ютерної стеганографії

У сучасній КС існує два основних типи файлів: повідомлення - файл, що призначений для приховування, і контейнер - файл, що може бути використаний для приховування в ньому повідомлення. При цьому контейнери бувають двох типів. Контейнер-оригінал (або "порожній" контейнер) - це контейнер, що не містить схованої інформації. Контейнер-результат (або "заповнений" контейнер) - це контейнер, що містить сховану інформацію. Під ключем розуміється секретний елемент, що визначає порядок занесення повідомлення в контейнер. Класичним є наступний принцип вбудовування даних [1,2]. Нехай сигнал контейнера представлений послідовністю з N біт. Процес приховання інформації починається з визначення біт контейнера, які можна змінювати без внесення помітних спотворень — стеганошляху. Далі серед цих біт, зазвичай у відповідності до ключа, обираються біти, що замінюються бітами приховуваного повідомлення.

Базовими положеннями сучасної КС є:

1. Забезпечення автентичність і цілісність файлу.
2. Обізнаність супротивника з можливостями КС.
3. Безпека ґрунтується на збереженні стеганографічним перетворенням основних властивостей переданого файлу при внесенні в нього секретного повідомлення і деякої невідомої супротивникові інформації - ключа.
4. Витяг секретного повідомлення має становити складну обчислювальну задачу.

Огляд стеганографічних методів і їх класифікація

Сучасні методи КС розвиваються у двох основних напрямках: 1) мето-

ди, засновані на використанні спеціальних властивостей комп'ютерних форматів; 2) методи, засновані на надмірності аудіо і візуальної інформації.

Більшість методів КС базується на двох принципах:

1) файли, які не вимагають абсолютної точності (наприклад, файли з зображенням, звуковою інформацією тощо), можуть бути видозмінені (до певного ступеня) без втрати своєї функціональності;

2) органи чуття людини не здатні надійно розрізняти незначні зміни у модифікованих таким чином файлах та/або відсутній спеціальний інструментарій, який був би спроможним виконати дану задачу.

Існуючі методи КС можна класифікувати (рис.1), спираючись на відомі публікації [1-7] та вибираючи той чи інший класифікаційний критерій.

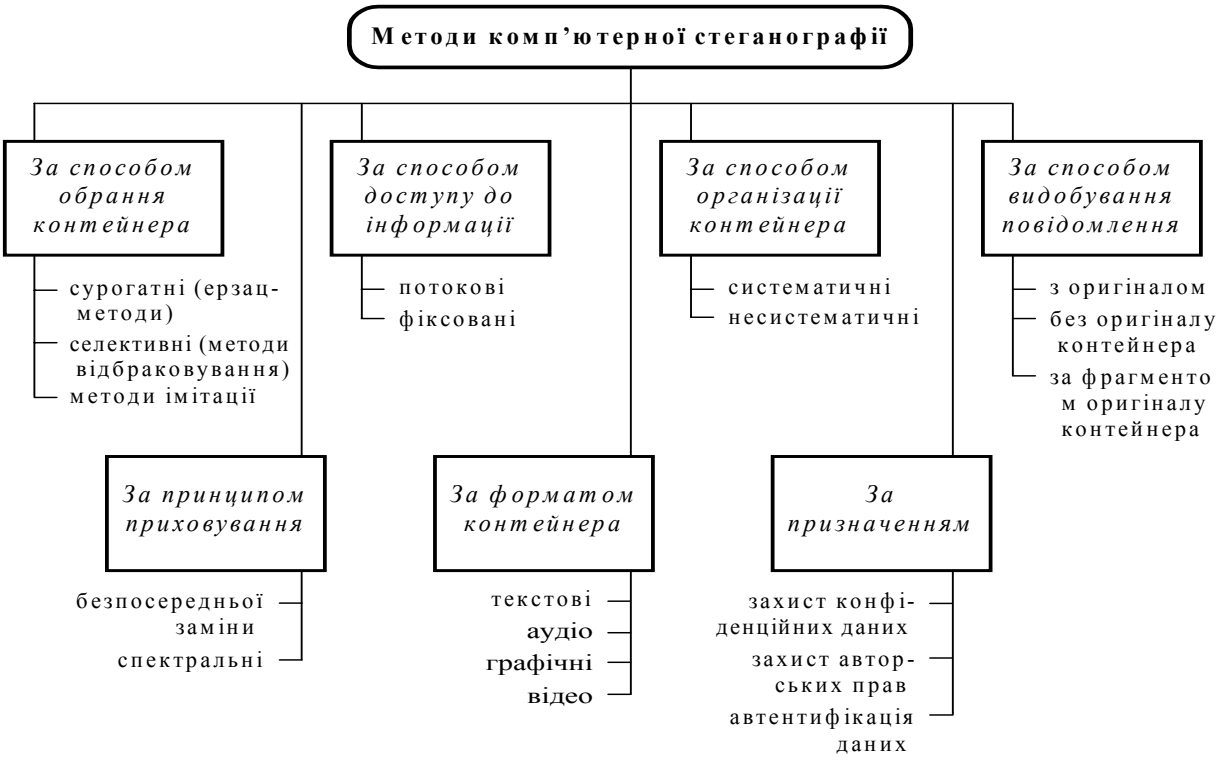

Рис.1. Класифікація методів комп'ютерної стеганографії.

За способом обрання контейнера розрізняють сурогатні, селективні та імітаційні методи стеганографії. В *сурогатних* (*безальтернативних*) методах стеганографії відсутня можливість вибору контейнера і для приховування повідомлення вибирається перший контейнер, що трапився, який у більшості випадків не є оптимальним для приховуваного повідомлення (так званий ерзац-контейнер). У *селективних* методах КС передбачається, що приховане повідомлення повинно відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів, з наступним обранням (шляхом відбраковування) найоптимальнішого з них для конкретного повідомлення. Окремим

випадком такого підходу є обчислення деякої хеш-функції для кожного контейнера. При цьому для приховання повідомлення обирається той контейнер, хеш-функція якого збігається зі значенням хеш-функції повідомлення (тобто стеганограмою є обраний контейнер). В *імітаційних* методах стеганографії контейнер генерується самою стеганосистемою. При цьому існують декілька варіантів реалізації. Так, наприклад, шум контейнера може імітуватися приховуваним повідомленням. Це реалізується за допомогою процедур, які не лише кодують приховане повідомлення під шум, але й зберігають модель початкового шуму. У граничному випадку за моделлю шуму може будуватися ціле повідомлення. Прикладом може слугувати метод, реалізований у програмі *MandelSteg* [5], яка в якості контейнера генерує фрактал Мандельброта (*Mandelbrot fractal*), або ж апарат функцій імітації [6].

За способом доступу до приховуваної інформації розрізняють методи *потокових* (*безперервних*) і фіксованих (*обмеженої довжини*) контейнерів.

За способом організації контейнери, подібно завадозахищеним кодам, можуть бути *систематичними* і *несистематичними*. У перших можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти власне контейнера, а де шумові біти, призначені для приховування інформації (як, наприклад, у широко поширеному методі найменшого значущого біту). У випадку несистематичної організації контейнера такий поділ не можливий. У цьому разі для виділення прихованої інформації необхідно обробляти вміст усієї стеганограми.

За використовуваним принципом приховування методи комп'ютерної стеганографії поділяють на два основних класи: методи *безпосередньої заміни* і *спектральні* методи. Якщо перші, використовуючи надлишковість інформаційного середовища в просторовій (для зображення) або часовій (для звуку) області, полягають в заміні малозначимої частини контейнера бітами секретного повідомлення, то другі для приховування даних використовують спектральне представлення елементів середовища, куди вбудовуються приховувані дані (наприклад, до різних коефіцієнтів дикретно-косинусних перетворень, перетворень Фур'є, Карунена-Лоева, Адамара, Хаара тощо).

Основним напрямком КС є використання властивостей саме надлишковості контейнера-оригінала. Але при цьому треба зважати на те, що при приховуванні інформації відбувається спотворення деяких статистичних властивостей контейнера або ж порушення його структури.

В особливу групу можна виділити методи, що використовують спеціальні властивості форматів представлення файлів [7]:

— зарезервовані для розширення поля файлів, які зазвичай заповнюються нулями і зазвичай не враховуються програмою;

— спеціальне форматування даних (зсування слів, речень, абзаців або обирання визначених позицій літер);

— використання незадіяних ділянок на магнітних та оптичних носіях;
— видалення файлових заголовків-ідентифікаторів тощо.

Для таких методів характерні низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

За призначенням розрізнюють стеганометоди власне для *прихованого передавання* (*прихованого збереження*) даних і методи для приховування даних у цифрових об'єктах з метою захисту авторських прав на них.

За типами контейнера виділяють стеганографічні методи із контейнерами у вигляді тексту, аудіофайлу, зображення та відео.

З огляду на зазначене запропоновано алгоритм організації приховування повідомлення наведений на рис.2.

Рис.2. Стеганографічний алгоритм приховування повідомлення.

Висновки і перспективи дослідження

Характерною тенденцією в даний час в області ЗІ є впровадження криптологічних методів. Однак на цьому шляху багато ще невирішених проблем, зв'язаних з руйнівним впливом на криптозасоби таких складових інформаційної зброї як комп'ютерні віруси, логічні бомби, автономні репликативні програми, т.п. Об'єднання методів КС і криптографії є гарним виходом з положення, що створилося. У цьому випадку можна усунути слабкі сторони відомих методів захисту інформації і розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки. Наведена схема класифікації і запропонований алгоритм приховування повідомлень, допоможуть наглядно оцінити можливості КС, спрощують написання стеганографічних програм для різних типів даних.

Література

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: "МК-Пресс", 2006. — 288 с.
2. Грибунин В.Г.,Оков И.Н.,Туринцев И.В. Цифровая стеганография.М.:Солон-Пресс, 2002.
3. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії : Навч. посіб. для студентів і аспірантів. — Вінниця: ВДТУ, 2003.
4. Генне О.В. Основные положения стеганографии.// Защита информации. №3, 2000.
5. N.F. Johnson, S. Jajodia, Steganalysis: The Investigation of Hidden Information, IEEE Information Technology Conference, Syracuse, New York, USA, Sept. 1st-3rd. 1998.
6. Інформаційний ресурс http://www.datapro.com.
7. Барсуков В.С., Романцов А.П. Компьютерная стеганография: вчера, сегодня, завтра. Технологии информационной безопасности XXI века. (http://st.ess.ru/).

Навроцкий Д.А. **Методы компьютерной стеганогарфии** Рассмотрены методы компьютерной стеганографии с точки зрения их классификации	Navrotsky D.A. **The methods computer steganography** The methods computer steganography from the view of their classification are considered