УДК 004.056

Горпенюк А.Я., Стороженко А.О.

Національний університет „Львівська політехніка”

кафедра захисту інформації

ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ДЛЯ ВПРОВАДЖЕННЯ ДАНИХ У ЦИФРОВІ ФАЙЛИ/RESEARCH AND COMPARATIVE ANALYSIS OF STENOGRAPHY METHODS FOR IMPLEMENTATION THE DATA INTO DIGITAL FILES

This article is dedicated to the analysis of steganography techniques that ensure privacy and integrity of hidden data. Also are considered the features of using these methods for copyright protection and covert communication.

Keywords - digital steganography, container, digital watermarks, covert communication.

Дана стаття присвячена аналізу стеганографічних методів, які забезпечують конфіденційність та цілісність прихованих даних. Також розглядаються особливості використання цих методів для захисту авторських прав і прихованого зв'язку.

Ключові слова - цифрова стеганографія, контейнер, цифрові водяні знаки, прихований зв'язок.

Вступ

Сучасні комп'ютерні технології обробки даних дозволили суттєво підвищити рівень інформаційної безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. Як відомо, на відміну від криптографічного захисту інформації, стеганографічні програмні засоби намагаються в першу чергу приховати сам факт існування конфіденційної інформації. Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на базі комп’ютерної техніки і програмного забезпечення складають предмет вивчення цифрової стеганографії.

Актуальність дослідження методів стеганографії невпинно росте, адже з поширенням персональних комп'ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу значної кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних [1–5]. Метою даної роботи є дослідження сучасних стеганографічних методів ЗІ, аналіз їхніх переваг та недоліків, аспектів їх практичного застосування.

Стеганографія та цифрові водяні знаки

Цифрова стеганографія — напрям класичної стеганографії, що полягає у впровадженні додаткової інформації у цифрові об'єкти (контейнери), викликаючи при цьому деякі спотворення цих об'єктів. Дана технологія призначена для організації таємного зв’язку, що є класичним завданням стеганографії, проте останнім часом вона використовується також для захисту інтелектуальної власності [3]. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації і полягає у вбудовуванні в об'єкт, що захищається, невидимих міток – цифрових водяних знаків (ЦВЗ) . На відміну від звичайних паперових водяних знаків ЦВЗ можуть бути не тільки видимими, але і , як правило, невидимими. Невидимі ЦВЗ аналізуються спеціальним

декодером, який виносить рішення про їх коректність. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або будь-яку іншу інформацію.

Основна відмінність задачі прихованої передачі даних від задачі вбудовування ЦВЗ полягає в тому, що в першому випадку порушник повинен здогадуватись про наявність прихованого повідомлення, тоді як у другому випадку його існування може не приховуватися [2].

Застосування методів стеганографії для різних завдань захисту інформації

Традиційно інтерес до стеганографічних методів проявлявся у військових і дипломатичних колах, оскільки донедавна термін «стеганографія» означав лише приховану передачу інформації. Сьогодні ж ця технологія знаходить своє застосування в інших сферах діяльності, пов'язаних з інформаційною безпекою. Зокрема існують методи, що дають можливість впровадження ЦВЗ у файли різних форматів, заголовки IP-пакетів, у текстові повідомлення та цифрові медіа-дані [1].

У Таблиці 1 наведено ряд завдань, які вирішують стеганографічні методи.

Таблиця 1.

Області застосування стеганографії	
Захист від копіювання Електронна комерція, контроль за копіюванням (DVD), розповсюдження мультимедійної інформації (відео за запитом)	**Прихована анотація документів** Медичні знімки, картографія, мультимедійні бази даних
Аутентифікація Системи відео-спостереження, електронної комерції, голосової пошти, електронне конфіденційне діловодство	**Прихований зв'язок** Військові та розвідувальні додатки

Однією з проблем, пов'язаних з ЦВЗ, є різноманіття вимог, що ставляться перед системою в залежності від завдань, які вона повинна вирішувати. Наприклад, співвідношення між ступенем захищеності вбудованого повідомлення та його розміром буде змінюватись в залежності від призначення стегосистеми. Для захисту авторських прав важливо, щоб водяний знак був стійкам до видалення чи спотворення, натомість об'єм інформації, яку він становить може бути невеликим. Для прихованого зв'язку, – навпаки, кількість переданої інформації є значно більшою. Менш важливою стає стійкість до модифікацій контейнера, вона повинна бути достатньою, щоб прочитати приховану інформацію.

На рис. 1 показана залежність, справедлива для всіх стеганографічних методів, при якій збільшення обсягу вбудованих даних значно знижує надійність системи [2].

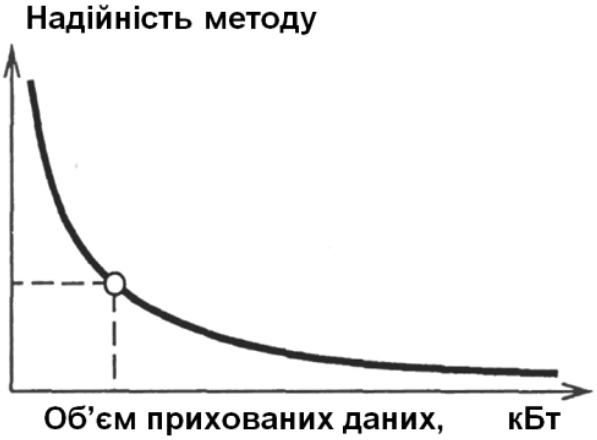

Рис. 1. Співвідношення між ступенем захищеності вбудованого повідомлення та його розміром.

Отже, в залежності від цілей, для яких використовується приховування даних, різними є і вимоги щодо рівня стійкості системи до модифікації контейнера. Як наслідок, для різних цілей оптимальними є різні методи стеганографії.

Аналіз існуючих стеганографічних методів

Елементам візуального середовища (цифровим зображенням і відео) властива значна надлишковість різної природи:

- кодова надлишковість,
- міжпіксельна надлишковість,
- психовізуальна залежність, зумовлена сприйманням органом зору людини зображення не в точності «піксель за пікселем», а з різною чутливістю.

Тому значна частина досліджень в області стеганографії присвячена методам приховування конфіденційних повідомлень і цифрових водяних знаків (ЦВЗ) у нерухомих зображеннях. На даний момент існує велика кількість методів приховування інформації і ЦВЗ у графічні файли.

Методи заміни в просторовій області. Класичним прикладом є метод заміни молодших біт (LSB- метод), який базується на тому, що молодші розряди графічних, аудіо і відео форматів несуть мало інформації і їх зміна практично не позначається на якості переданого зображення або звуку. Це дає можливість використання їх для кодування конфіденційної інформації [5].

Основною перевагою даного методу є простота реалізації та можливість таємної передачі великого об'єму інформації. Однак за рахунок введення додаткової інформації спотворюються статистичні характеристики файлу-контейнера і приховане повідомлення легко виявити за допомогою статистичних атак, таких як оцінка ентропії та коефіцієнтів кореляції. Для зниження компрометуючих ознак потрібна корекція статистичних характеристик. Недоліком методу є також його чутливість до операцій цифрової обробки: стиснення, застосування фільтрації, конвертації кольорів, геометричних перетворень, додаткового зашумлення та зміни формату контейнера.

У методах, що діють *в частотній області* дані приховуються у коефіцієнтах частотного представлення контейнера. Для цього найчастіше використовуються перетворення, які застосовуються у сучасних алгоритмах стиснення із втратами (дискретне косинусне перетворення в стандарті JPEG і вейвлет перетворення – в JPEG2000). Приховання інформації може проводитися як в початкове зображення, так і одночасно із здійсненням стиснення зображення-контейнера. Важливо, що стегосистеми, у яких враховані особливості алгоритму стиснення, є нечутливими до подальшої компресії контейнера. Також вони забезпечують більшу стійкість до геометричних перетворень і виявлення каналу передачі (порівняно з методом LSB), оскільки є можливість в широкому діапазоні варіювати якість стисненого зображення, що робить неможливим визначення походження спотворення [4].

Широкосмугові методи. Суть даних методів полягає в розширенні смуги частот сигналу, до ширини спектру , значно більшої ніж це необхідно для передачі реальної інформації. Для розширення діапазону існують два способи: метод прямого розширення спектру, за допомогою псевдо – випадкової послідовності, і метод стрибкоподібного переналаштування частоти. При цьому корисна інформація розподіляється по всьому діапазону, тому при втраті сигналу в деяких смугах частот в інших смугах залишається достатньо інформації для її відновлення. Принцип дії широкосмугових методів споріднений із завданнями, які вирішують стегосистеми: спробувати "розчинити" секретне повідомлення в контейнері і зробити неможливим його виявлення [5].

Оскільки сигнал, розподілений по всій смузі спектра, його важко виділити. Це є суттєвою превагою даних методів, як і стійкість до випадкових та умисних спотворень. Тому вони застосовуються в техніці зв'язку для забезпечення високої завадостійкості і складності процесу перехоплення та виявлення. Натомість недоліком є можливість стегоаналізу за рахунок цифрової обробки з використанням шумозгладжуючих фільтрів.

Статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення. Наприклад, ідея алгоритму Patchwork базується на припущенні, що значення пікселів незалежні і однаково розподілені. При цьому генерується секретний ключ для ініціалізації генератора псевдовипадкових чисел, які вказують на місце в зображенні, куди вносяться біти водяного знака. Для цього у відповідності зі стегоключем вибирається n пар пікселів (a_i,b_i) у яких значення яскравості змінюється в такий спосіб:

$$\bar{a} = ai + 1\,,\ \ \bar{b} = bi + 1 \tag{1}$$

Під час виділення водяного знака обчислюється сума:

$$Sn = \sum_{i=1}^{n} \left(\bar{a}_i - \bar{b}_i\right) \tag{2}$$

Якщо Sn значно відрізняється від нуля, виноситься рішення про наявність ЦВЗ [5]. Даний метод забезпечує високу стійкість до операцій цифрової обробки, та важкість виявлення прихованих даних без відповідного секретного ключа.

Таким чином результати дослідження показують, що надійність методів заміни в просторовій області залежить від рівня частотних спотворень контейнера. Разом з тим вони забезпечують високу швидкодію і значний обсяг вбудованих даних, тому їх доцільно використовувати при передачі прихованих повідомлень. Методи, що діють в частотній області є стійкішими до спотворень та операцій цифрової обробки, але можуть приховати менший об’єм даних. Наявність секретного ключа у широкосмугових та статистичних методах, що використовують псевдовипадкове кодування, підвищує їх надійність. А розподіл прихованих біт по всьому контейнері зумовлює високу стійкість до випадкових та умисних спотворень, що враховується при побудові ЦВЗ.

Висновок

У даній статті розглянуто ряд методів, що використовуються для стеганографічного захисту інформації, виділено їх основні характеристики, переваги й недоліки. В процесі досліджень було виявлено клас задач захисту, що можуть мати ефективне вирішення за допомогою методів цифрової стеганографії. Також здійснено порівняльний аналіз цих методів, який показав, що методи заміни у просторовій та частотній областях доцільніше використовувати для прихованого зв’язку, а в технологіях ЦВЗ ефективнішим буде застосування широкосмугових та статистичних методів.

Література

1. Грибунин В.Г. Цифровая стеганография. / В. Г. Грибунин, И.Н. Оков, И.В. Туринцев. – К.: Солон-Пресс, 2002. – 265 с. 2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика. / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с. 3. Поліновський В.В. Інформаційна технологія для досліджень методів стеганографії і стегоаналізу / В.В. Поліновський // Міжвузівський збірник "Комп'ютерно-інтегровані технології: освіта, наука, виробництво ". – Луцьк, 2011. - №5 – с.236-242. 4. Таранчук А.А. Стеганографічний метод приховування даних в області частотних перетворень зображень / А.А. Таранчук, Л.Г. Гальпер // Вісник Хмельницького національного Університету. – Хмельницький, 2009. – № 2 "Технічні науки" – С.197-201. 5. Хорошко В.А. Методи й засоби захисту інформації. / В.А. Хорошко, А. А. Чекатков. – К.: Юніор, 2003. – 504 с.