УДК 004.056 (621.3)

В.О.Денисюк
Вінницький національний аграрний університет
А.В.Денисюк
Вінницький національний технічний університет

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ДАНИХ З ВИКОРИСТАННЯМ ФАЙЛІВ ЗОБРАЖЕНЬ

Дуже часто при зберіганні інформації, а особливо інформації економічного або технологічного спрямування, виникає потреба у її приховуванні від сторонніх очей. Чим більша цінність інформація тим більшого захисту вона потребує. Наприклад, такі прибуткові та розвинуті компанії як Apple або Samsung доводять різноманітними засобами у тому числі і судовими позивами, що використані ними технології є неповторними та інноваційними, що їхні права на використання цих можливостей є автономними. Відповідну інформацію можна використовувати для здобуття надприбутків та випереджаючого розвитку певних галузей. Для гарантованого захисту вмісту повідомлення існує два різних підходи. Перший пов'язаний з блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення. Другий підхід полягає у тому, що повідомлення, яке передається, намагаються приховати так, аби його неможливо було знайти. За першим підходом використовують криптографічні методи захисту. У криптограмах, як правило, відсутні структура і закономірності, які властиві відкритим текстам. Тому, при проведенні моніторингу мереж телекомунікацій, вони легко автоматично виділяються з інформаційного потоку. Другий підхід застосовує стеганографічні методи захисту, які значно знижують ймовірність її виявлення. На відміну від криптографічного захисту, коли у «зловмисника» існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати інформацію, що передається, в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту. Шанси знайти приховане повідомлення невеликі, але на той випадок, якщо повідомлення буде виявлено, його можна ще додатково зашифрувати. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Не існує абсолютно надійного способу зашифрувати інформацію. Кращий спосіб захистити її - це приховати сам факт її існування. Цим стеганографія перевершує криптографію [1]. Метою роботи є підвищення рівня захисту інформації від несанкціонованого доступу за рахунок приховування її у мультимедійних файлах.

Аналіз сучасного стану у розвитку стеганографії окреслив її основні завдання [2]:

1) захист конфіденційної інформації від несанкціонованого доступу;
2) подолання систем моніторингу та управління мережевими ресурсами;
3) камуфлювання програмного забезпечення;

4) захист авторського права на деякі види інтелектуальної власності.

Найбільш ефективна задача стеганографії – захист інформації. Так, наприклад, одна секунда оцифрованого звуку з частотою дискретизації 44100Гц і рівнем відліку в 8 біт у стереорежимі дозволяє приховати за рахунок зміни найменш значимих молодших розрядів повідомлення у 10 Кбайт. Такий підхід дозволяє досягти змін у 1%, яких людина при прослуховуванні не здатна помітити, але при розшифруванні чи зчитуванні певним чином, дозволяє зберегти інформацію. Цей приклад дає ілюстрацію можливостей стеганографії. Також треба зазначити, що без спеціальних засобів збережену інформацію не можливо отримати із файла-контейнера.

Також, стеганографічні методи, спрямовані на протидію системам моніторингу та управління мережевими ресурсами промислового шпигунства, дозволяють протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери керування локальних і глобальних обчислювальних мереж. Для корпорацій та державних відомств, що зберігають важливі масиви даних, це одна із неоціненних функції стеганографії.

Іншим важливим завданням стеганографії є камуфлювання програмного забезпечення (ПЗ). У тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано в файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Прикладом використання стеганографії у захисті авторського права від піратства є нанесення спеціальної мітки на комп'ютерні графічні зображення. Мітка залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням. Таке програмне забезпечення вже використовується в комп'ютерних версіях деяких журналів. Даний напрямок стеганографії призначений не тільки для обробки зображень, але і для файлів з аудіо- та відеоінформацією та забезпечює захист інтелектуальної власності.

На тепер важливим і перспективним є кожне із наведених завдань стеганографії, сучасне розуміння проблеми захисту інформації та її безпеки полягає у подальшому розвиткові цього питання і шляхів його вирішення, які ця наука може запропонувати. Різноманітні стегано-алгоритми дозволяють в тій чи іншій мірі задовольнити завданням конфіденційності [3].

В даний час найбільш поширеним, але найменш стійким є метод заміни найменших значущих бітів або LSB-метод (Least Significant Bit, найменший значущий біт). Він полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих зображеннях або аудіо- і відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація молодших бітів в більшості випадків не викликає значної трансформації зображення і не виявляється візуально.

Іншим популярним методом вбудовування повідомлень є використання особливостей форматів даних, що застосовують стиснення з втратою даних

(наприклад JPEG). Цей метод (на відміну від LSB) більш стійкий до геометричних перетворень і виявленню каналу передачі, так як є можливість в широкому діапазоні варіювати якість стислого зображення, що робить неможливим визначення походження спотворення, але його складніше використовувати для приховування великих повідомлень.

Не менш поширеним методом передачі прихованої інформації, є мімікрія. Мімікрія генерує текст, використовуючи синтаксис і Contex Free Grammar (CFG – один із способів опису мови, яка складається з синтаксичних слів, фраз, вузлів, де може бути прийнято рішення, яке слово чи фразу далі вставляти в текст). Мімікрія створює бінарне дерево, яке базується на можливості CFG, і будує текст, обираючи ті з гілок дерева, які кодують кожний біт. Недоліком цього методу є неможливість передачі великих об'ємів інформації, низка продуктивність методу і невисокий ступінь захисту.

Є ще кілька алгоритмів роботи з графічними файлами. Наприклад, метод розширення палітри, що працює тільки для структури GIF. Він є найбільш ефективний в зображеннях з палітрою невеликих розмірів. Його суть у тому, що збільшується розмір палітри аби надати додатковий простір для запису необхідних байт на місці байт кольорів. При мінімальній палітрі 2 кольори (6 байт) максимальний розмір повідомлення може бути 256×3-6=762 байт. Недолік - низька криптозахищеність, прочитати заховане повідомлення можна за допомогою будь-якого текстового редактора, якщо повідомлення додатково не шифрувалося [4].

Отже, методи, що використовують графічні файли, є найбільш вигідними і перспективними, оскільки немає обмежень по об'єму переданих даних, все залежить від підібраного контейнеру. Також тут присутній високий ступінь захисту. У якості основного стегано-алгоритму є сенс використовувати LSB-алгоритм. Він дозволяє зробити таку заміну, яка в загальному випадку не помітна людському оку. Більш того, багато старих пристроїв виведення, навіть не зможуть відобразити такі незначні зміни. Також можна змінювати не тільки два молодших біта, але і будь-яку їх кількість. Тут є наступна закономірність - чим більшу кількість бітів замінюється, тим більший обсяг інформації можна заховати, але тим більші завади будуть у вихідному зображенні.

Література:

1. Вікіпедія – Вільна енциклопедія [Електронний ресурс]: Стеганографія.– Режим доступу: http://ru.wikipedia.org/wiki/

2. Бюро науково-технічної інформації [Електронний ресурс]: Комп'ютерна стеганографія вчора, сьогодні, завтра. – Режим доступу: http://www.bnti.ru/

3. Ярмолик С.В. Стеганографические методы защиты информации [Текст] / С. В. Ярмолик, Ю. Н. Листопад // Информатизация образования. - 2005. - № 1. - С. 64-74.

4. Стеганографія [Електронний ресурс]: - Стеганографія в GIF. – Режим доступу: http://habrahabr.ru/post/128327/