УДК 621.396

О.А. Смірнов

Кіровоградський національний технічний університет, Кіровоград

ДОСЛІДЖЕННЯ СТЕГАНОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ ДЛЯ ОРГАНІЗАЦІЇ СКРИТНИХ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

Розглядається процес стеганографічного перетворення інформації за відповідними етапами. Досліджуються властивості та введено класифікацію стеганоконтейнерів.

Ключові слова: *стеганографія, захист інформації, стеганоконтейнер.*

Вступ

Методи скритної передачі цифрової інформації і, зокрема, сучасні засоби стеганографічного приховування даних в просторовій області зображень є на сьогодні одним із перспективних напрямків розвитку механізмів захисту інформації [1 – 5]. Їх основною перевагою є можливість приховування не тільки смислового змісту інформаційних даних, а й самого факту організації таємної передачі повідомлень. Це надає додаткові можливості з організації скритного управління та передачі цифрової інформації, в тому числі в військовій, дипломатичній та фінансово-економічній галузях.

Метою даної роботи є дослідження основних етапів стеганографічного перетворення інформації, введення основних понять та визначень.

1. Процес стеганографічного перетворення інформації

На поточний час існують наступні області застосування стеганографії:

– вбудовування інформації з метою приховання незаконної передачі даних;

– захист інформації від несанкціонованого доступу;

– вбудовування цифрових водяних знаків для захисту авторських прав (watermarking);

– вбудовування ідентифікаційних номерів (fingerprinting);

– вбудовування заголовків (captioning);

– камуфляж програмного забезпечення.

Цифрові водяні знаки (ЦВЗ) застосовуються для захисту від копіювання й несанкціонованого використання мультимедійної інформації й полягає у вбудовуванні в захищаємий об’єкт невидимих міток – ЦВЗ. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або яку-небудь керуючу інформацію. Найбільш підходящими об'єктами захисту за допомогою ЦВЗ є нерухливі зображення, файли аудіо- та відеоданих.

Технологія вбудовування ідентифікаційних номерів виробників має багато загального з технологією ЦВЗ. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікально вбудовуваний номер, (звідси й назва – дослівно «відбитки пальців»). Цей ідентифікаційний номер дозволяє виробнику відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то «відбитки пальців» швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту тощо. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній порушник.

Нерідко методи стеганографії використовують для камуфлювання програмного забезпечення. У тих випадках, коли використання програм незареєстрованими користувачами є небажаним, воно може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

При використанні методів стеганографії повинні враховуватися наступні умови:

– зловмисник може мати повне уявлення про стеганографичну систему й деталі її реалізації. Єдиною інформацією, що повинна залишатися йому невідомою, – це ключ, за допомогою якого можна встановити факт присутності прихованого повідомлення і його зміст;

– якщо зловмиснику якимось чином вдалося довідатися про факт існування прихованого повідомлення, то це не повинно дозволити йому витягти подібні повідомлення з інших стеганограм доти, поки ключ зберігається в таємниці;

– потенційний зловмисник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

Більшість методів комп'ютерної стеганографії базується на наступних принципах.

Перший полягає в тому, що файли, які не вимагають абсолютної точності (наприклад, файли із зображенням, звуковою інформацією та ін.), можуть бути до певного ступеня видозмінені без втрати функціональності.

Другий принцип заснований на відсутності спеціального інструментарію або нездатності орга-

нів відчуттів людини надійно розрізняти незначні зміни в таких вихідних файлах.

За використовуваними принципами стеганометоди можна розбити на два класи: цифрові методи й структурні методи. Якщо цифрові методи стеганографії, використовуючи надмірність інформаційного середовища, в основному, маніпулюють із цифровим поданням елементів середовища, куди вбудовуються приховувані дані (наприклад, у пікселі, у різні коефіцієнти косинусних перетворень, перетворень Фур'є, Уолша-Радемахера або Лапласа), то структурні методи стеганографії для приховання даних використовують семантично значимі структурні елементи інформаційного середовища.

Основним напрямком комп'ютерної стеганографії є використання властивостей надмірності інформаційного середовища. Варто зазначити, що при прихованні інформації відбувається видозмінення деяких статистичних властивостей середовища або порушення її структури, які необхідно враховувати для зменшення демаскуючих ознак.

В особливу групу можна також виділити методи, які використовують спеціальні властивості форматів подання файлів:

– зарезервовані для розширення поля комп'ютерних форматів файлів, які звичайно заповнюються нулями й не враховуються програмою;

– спеціальне форматування даних (зсув слів, речень, абзаців або вибір певних позицій букв);

– використання незадіяних місць на магнітних носіях;

– видалення ідентифікуючих заголовків для файлу.

В основному, для таких методів характерний низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

Процес перетворення даних (повідомлення, ЦВЗ, заголовка або ідентифікаційного номера) в стеганографічній системі формально можливо розділити на наступні етапи (рис. 1).

Вбудовані дані, сформовані джерелом інформації, заздалегідь обробляються (кодуються), з метою їх підготовки і відображення в найбільш зручному вигляді. На цьому етапі можуть застосовуватись методи перешкодостійкого кодування інформації (якщо, наприклад, процес вилучення повідомлення на приймальній стороні має імовірнісний, стохастичний характер і потрібно підвищити імовірність правильного вилучення, тобто забезпечити заданий рівень достовірності передачі даних).

Цифровий контейнер (надмірні цифрові дані, в які буде вбудовано інформаційне повідомлення) формується джерелом контейнерів і аналізується на предмет прихованих особливостей, визначених його внутрішньою природною надмірністю.

Стеганографічне кодування складається у внесенні по певному алгоритму підготованих інформаційних даних до цифрового контейнера з урахуванням виявлених особливостей. Це найбільш важливий і відповідальний етап перетворення даних в стеганографічній системі захисту інформації, який виконується під управлінням секретних ключових даних (формованих джерелом ключів). З одного боку, вбудовані дані не повинні бути виявлені неуповноваженим користувачем без знання деяких секретних параметрів вбудовування (ключових даних), з іншого боку, сам факт вбудовування не повинен бути виявлений супротивником, тобто спотворення що вносяться, початкового (порожнього) контейнера, повинні бути мінімізовані.

Після передачі заповненого контейнеру (стеганограми) на приймальній стороні виконується стеганографічне декодування, тобто виконується процедура, зворотна стеганографічному кодуванню на передавальній стороні. Алгоритм декодування виконується під управління ключових даних і може принципово відрізнятися від процедури кодування (самі ключові дані для вилучення повідомлення можуть відрізнятися від ключових даних для вбудовування. В цьому випадку стеганосистема є несиметричною (асиметричною) і може бути побудована аналогічно відкритої криптографії).

Мета стеганографічного декодування полягає у формуванні деякої «оцінки» вбудованого повідомлення, тобто із заповненого контейнера вилучаються дані, які ймовірно можуть бути вбудованим повідомленням. Ця «оцінка» обробляється стеганодетектором, який видає рішення про її приналежність до множини можливих (припустимих) повідомлень. Іншими словами, стеганодетектор виконує найважливішу функцію стеганографічної системи захисту інформації – він ухвалює рішення про наявність або відсутність в прийнятому контейнері вбудованого повідомлення.

Вилучена «оцінка» інформаційного повідомлення, надходить на декодування вбудованих даних. На цьому етапі при позитивному вирішенні детектора, тобто при ухваленні рішення про наявність в контейнері вбудованих даних, виконуються перетворення, зворотні попередньому кодуванню на передавальній стороні. Іншими словами, вилучені з контейнера дані перетворяться до вигляду, найбільш зручного для одержувача інформації. Якщо на передавальній стороні застосовувалися методи перешкодостійкого кодування, тоді на приймальній стороні на цьому етапі перетворень виконується перешкодостійке декодування. Змінені на останньому етапі обробки дані надходять до одержувача інформації.

Розглянемо поняття цифрового контейнера і введемо загальну класифікацію контейнерів по найбільш природних ознаках.

2. Визначення та класифікація стеганоконтейнерів

Під контейнером розуміється послідовність цифрових даних, що мають, як правило, аналогову природу і що володіють природною внутрішньою надмірністю, в яких вбудовується інформаційне повідомлення.

Введемо наступну класифікацію контейнерів.

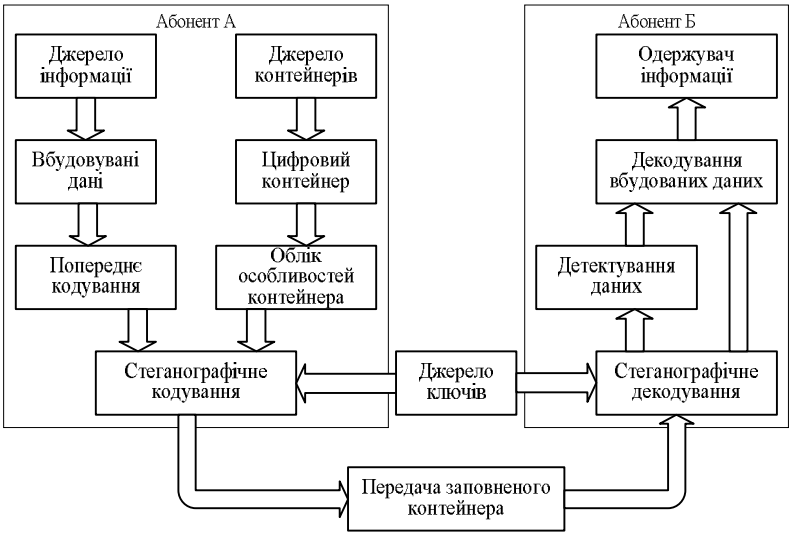

Рис. 1. Процес перетворення даних в стеганографічній системі

1. За способом формування:

– вибрані, коли відправник має можливість самостійно формувати контейнери або вибирати найбільш відповідні з деякої кількості контейнерів. Приклад: відібрані для відправки по електронній пошті фотографії і т.ін. Найбільш зручний для відправника вид контейнерів, не припускає доступ супротивника до процесу формування контейнерів. Вибраний контейнер може завісити від вбудованого повідомлення, а також бути його функцією.

– випадкові, коли відправник не має можливості впливати на процес формування контейнерів, а може використовувати тільки випадково сформовані деяким стохастичним процесом дані. Приклад: зображення, отримані в ході зйомки поверхні землі бортовою апаратурою штучного супутника; дані телеметрії що передаються і ін.

– нав'язані, коли відправник вимушений використовувати контейнери, сформовані або відібрані зловмисником, або контейнери, сформовані деяким детермінованим процесом до управління яким у відправника немає доступу. Наприклад, передача розвідувальній інформації в стеганографічному каналі, утвореному за допомогою вбудовування даних в радіограми супротивника (якщо, зрозуміло, у відправника є доступ до цих радіограм). Нав'язаний контейнер може з'явитися в сценарії, коли особа, що надає контейнер, підозрює про можливе приховане листування і бажає запобігти їй.

2. За фізичною природою використовуваної надмірності:

– рухливі (відео) зображення;

– нерухомі (фото) зображення;

– звукові сигнали;

– текстові документи;

– сигнали телеметрії і ін.

3. За типом цифрових даних:

– фіксовані, тобто що мають кінцевий розмір контейнери. Наприклад, цифрові фотографії, аудіо- або відеофайли, текстові документи. У фіксованого контейнера розміри і характеристики заздалегідь відомі. Це дозволяє здійснювати вкладення даних оптимальним в деякому розумінні чином.

– потокові, коли дані, використовувані для вбудовування інформації, мають вид безперервного цифрового потоку. Наприклад, канали цифрового телебачення і/або радіомовлення (не плутати з відео і аудіо файлами кінцевого розміру). Потоковий контейнер є безперервною послідовністю біт. Повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. У один контейнер великого розміру може бути вбудовано і декілька повідомлень. Інтервали між вбудовуваними бітами визначаються генератором псевдовипадкової послідовності з рівномірним розподілом інтервалів між відкликами. Основна складність полягає в здійсненні синхронізації, визначенні початку і кінця послідовності. Якщо в даних контейнера є біти синхронізації, заголовки пакетів і так далі, то прихована інформація може йти відразу після їх. Складність забезпечення синхронізації перетворюється на позитивну якість з погляду забезпечення прихованості передавання. Крім того, потоковий контейнер має велике практичне значення: уявіть собі, наприклад, стегоприставку до звичайного телефону. Під прикриттям звичайної телефонної розмови можна було б передавати іншу розмову, дані і тому подібне, і не знаючи секретного ключа не можна було б не тільки дізнатися зміст прихованої передачі, але і сам факт її існування. Не випадково, що робіт, присвячених розробці стегосистем з потоковим контейнером практично не зустрічається

Висновки

В ході проведених досліджень було розглянуто процес стеганографічного перетворення інформації за відповідними етапами, досліджено властивості та введено класифікацію стеганоконтейнерів. Перспективним напрямком подальших досліджень є створення інформаційних технологій стеганографічного перетворення інформації, дослідження кількісних та якісних показників ефективності стеганосистем.

Список літератури

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

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.

3. Хорошко В.А. Введение в компьютерную стеганографию / В.А. Хорошко, М.Е. Шелест. – К., 2002. – 140 с.

4. Smith J.R. Modulation and information hiding in images / J.R. Smith, B.O. Comisky // R. Anderson, editor, Information Hiding, First International Workshop, vol.1174 of Lecture Notes in Computer Science. – Springer-Verlag, Berlin, 1996. – P. 207-226.

5. Marvel L.M. Spread Spectrum Image Steganography / L.M. Marvel, C.G. Boncelet, C.T. Retter // IEEE Transactionson Image Processing. – Vol 8, No 8. – August 1999. – P.1075-1083.

Надійшла до редколегії 11.01.2012

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИОННЫХ СООБЩЕНИЙ ДЛЯ ОРГАНИЗАЦИИ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

А.А. Смирнов

Рассматривается процесс стеганографического преобразования информации по соответствующим этапам. Исследуются свойства и введена классификация стеганоконтейнеров.

Ключевые слова: *стеганография, защита информации, стеганоконтейнер.*

RESEARCH OF steganography OF TRANSFORMATION OF INFORMATION MESSAGES FOR ORGANIZATION OF THE HIDDEN CHANNELS OF DATA

A.A. Smirnov

The process of steganography transformation of information is examined on the corresponding stages. Properties are investigated and classification of steganocontainer is entered.

Keywords*: steganography, protection to information, steganocontainer.*