УДК 003.26:004.056.55
С 17

ВИКОРИСТАННЯ МЕТОДІВ ДИНАМІЧНОЇ СТЕГАНОГРАФІЇ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Д. М. Самойленко, канд. фіз.-мат. наук, доц.;
К. М. Новосьолова, студ.

Національний університет кораблебудування, м. Миколаїв

Анотація. Проаналізовано особливості використання стеганографічних методів у модулях перевірки автентичності інформаційних ресурсів. Запропоновано методику динамічної стеганографії з текстовим стегоконтейнером.
Ключові слова: динамічна стеганографія, цифрові водяні знаки, автентичність.

Аннотация. Проанализированы особенности применения стеганографических методов в модулях проверки подлинности информационных ресурсов. Предложена методика динамической стеганографии с текстовым стегоконтейнером.
Ключевые слова: динамическая стеганография, цифровые водяные знаки, подлинность.

Abstract. The steganographic methods in authentication modules of information resources have been analyzed. The dynamic steganographic method with a text stego-container has been proposed.
Keywords: dynamic steganography, digital watermarks, authenticity.

ПОСТАНОВКА ПРОБЛЕМИ

Сучасна стеганографія об'єднує у собі сукупність методів, які ґрунтуються на принципах приховування самого факту існування таємної інформації в тому або іншому середовищі – контейнері. Прогрес у галузі глобальних комп'ютерних мереж і засобів мультимедіа привів до розробки нових методів, призначених для забезпечення безпеки передачі даних по каналах телекомунікацій, і використання їх в неоголошених цілях.

Більшість таких методів ураховують природні неточності пристроїв оцифровування і надмірність аналогового відео- або аудіосигналу, чим дозволяють приховувати повідомлення в комп'ютерних файлах. Причому, на відміну від криптографії, дані методи приховують сам факт передачі інформації.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Стеганографічні методи використовуються, в основному, для передачі повідомлень невисокої важливості [1]. Для стеганографічних методів не застосовують принципи Керкгоффса, які висуваються до криптографічних систем і вимагають вільного поширення інформації про криптографічні перетворення. Відповідно, уся надійність стеганографічних систем полягає у таємності самих алгоритмів внесення інформації до контейнерів. Дискредитація стеганографічної системи призведе до неможливості подальшого використання цієї системи у режимі таємності. Однак для передавання інформації з невисокою цінністю можлива межа, коли цінність дискредитації системи буде більшою за цінність інформації. Для такої малоцінної інформації знаходить застосування більшість сучасних комп'ютерних стеганографічних методів [1].

З іншого боку, приховування факту наявності інформації може бути використано як захисний засіб для інформаційного ресурсу. У ситуації коли можливі появи клонів інформаційних ресурсів, прихована інформація може слугувати ідентифікатором автентичності ресурсу.

Головна ідея впровадження стеганографічних методів у модулі автентифікації інформаційних ресурсів полягає у включенні певної прихованої інформації у візуальні або мультимедійні складові частини інформаційного ресурсу. Більшість відомих стеганографічних методів можна класифікувати за наступними ознаками [2]:

1) методи, засновані на використанні спеціальних властивостей комп'ютерних форматів;

2) методи, засновані на надмірності візуальної та аудіоінформації.

Перший напрямок базується на використанні спеціальних властивостей комп'ютерних форматів представлення даних. Спеціальні властивості форматів вибираються з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або прочитання.

Другий напрямок заснований на використанні надмірності візуальної та аудіоінформації (цифрові фотографії, цифрова музика і цифрове відео).

До окремого класу стеганографічних методів можна віднести засоби текстової стеганографії або так звані цифрові «водяні» знаки.

МЕТОЮ СТАТТІ є розроблення методики для адаптування стеганографічних методів до задач підтвердження автентичності інформаційних ресурсів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для застосування у задачах підтвердження автентичності слід обрати методи, які подібно до контейнерів використовують об'єкти, типово присутні на доступних частинах інформаційного ресурсу – на сайті. До таких об'єктів можна віднести:

– статичні графічні об'єкти (рисунки, логотипи, рекламні банери тощо);

– динамічні графічні об'єкти (відеоконтент, рухома реклама тощо);

– текстові поля (новини, загальні вітання, основна інформація, рекламні та технічні характеристики тощо);

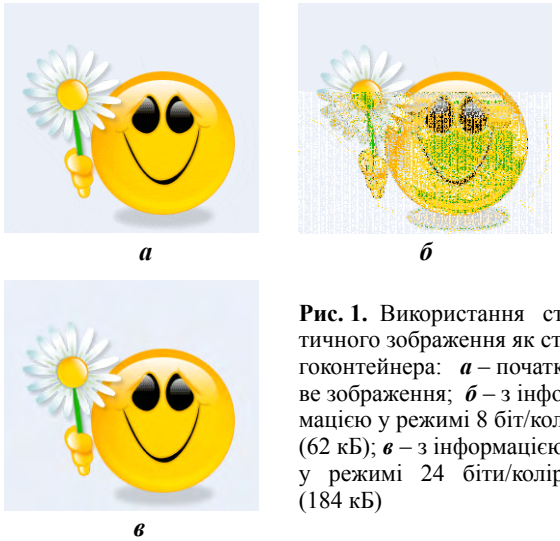
– прикріплені файли.

Найменш зручними з точки зору захисних рішень є прикріплені файли. Спрямовуючи зусилля на клонування або віддзеркалення інформаційних ресурсів, зловмисник може легко забезпечити завантаження потрібних файлів, навіть не намагаючись дискредитувати стеганографічні алгоритми.

Як статичні, так і динамічні графічні об'єкти забезпечують захист лише у тому разі, коли на клієнтській частині інформаційного ресурсу встановлені засоби коректного відображення відповідних об'єктів (плагіни), а також коли клієнтом не відключено їх відображення, що може здійснюватися з метою прискорення інформаційного обміну чи запобігання відображенню рекламної інформації. Наявність додаткових графічних об'єктів неочевидного призначення також може викликати певні підозри щодо включення цих об'єктів до візуальної частини ресурсу. Логічним графічним елементом інформаційного ресурсу може бути логотип установи чи організації, якій належить ресурс.

Проте для непомітного введення додаткової інформації зображення повинно мати достатню надмірність. На рис. 1 подано результати стеганографічної інтервенції однакової інформації у зображення з різною розрядністю подання кольору. Як видно з рисунка, при розрядності 8 біт на колір спотворення зображення стає помітним навіть при зміні лише одного молодшого біта кольору. При розрядності 24 біти на колір зміни зображення не помітні, проте розмір зображення збільшується майже втричі. При прагненні скорочення розмірів об'єктів, присутніх в інформаційних ресурсах, використання зображення з високою кольоровою розрядністю саме по собі може викликати підозри.

Більш універсальним стеганографічним контейнером для інформаційного ресурсу можна вважати текстові поля. Текстова інформація є основною для більшості інформаційних ресурсів. У будь-якому разі наявність текстової інформації не повинна викликати жодних підозр щодо її нелогічного, нав'язливого розміщення у візуальній складовій ресурсу.



а ***б*** ***в***

Рис. 1. Використання статичного зображення як стегоконтейнера: ***а*** – початкове зображення; ***б*** – з інформацією у режимі 8 біт/колір (62 кБ); ***в*** – з інформацією у режимі 24 біти/колір (184 кБ)

Серед найбільш поширених методів текстової стеганографії можна виділити певний базис з трьох методів:

– метод зміни порядку маркерів кінця рядка;

– метод кінцевих пробілів;

– метод знаків однакової форми.

Комбіновані методи можна розглядати як змішане використання базисних методів у рамках одного документа. Розглянемо особливості застосування окремих методів для поставленої задачі.

Метод зміни порядку маркерів кінця рядка використовує індиферентність більшості засобів відображення текстової інформації до порядку слідування символів переведення рядка (CR) та повернення каретки (LF), які обмежують рядок тексту. Можна вважати, що традиційний порядок слідування CR/LF відповідатиме біту 0, а інвертований LF/CR – біту 1 прихованого стеганографічного повідомлення.

Головним недоліком методу зміни порядку маркерів кінця рядка є мала ємність текстових контейнерів щодо зазначеного способу інтервенції. Текстове наповнення інформаційних ресурсів, як правило, не має великих обсягів, відповідно, маркерів кінця рядка у зазначених текстах небагато. Якщо вжити заходів щодо навмисного збільшення вказаних маркерів додаванням їх до кожного рядка (замість абзацу), то може постраждати форматування текстів особливо при масштабуваннях області відображення. Можна стверджувати, що метод зміни порядку маркерів кінця рядку слід використовувати для великих текстів або текстових файлів застарілих консольних редакторів (на зразок Лексикону), в яких маркери кінця рядка використовувалися наприкінці кожного рядка тексту.

Метод кінцевих пробілів передбачає дописування декількох пробілів у кінці коротких рядків. Метод може використовуватися у скороченій формі, коли наявність пробілу кодує біт 1, а відсутність – біт 0, та у розширеній формі, коли кількість пробілів кодує

відразу кількабітові числа (наприклад, від 0 до 7 пробілів кодує трибітову групу 000-111). Описаний метод, подібно до попереднього, має невелику ємність, обмежену кількістю абзаців у тексті, і стає чутливим до проявлення при масштабуванні, якщо додавати пробіли до кінця всіх рядків, які відображаються у певному масштабі. Область використання методу кінцевих пробілів припускається подібною до області використання методу зміни порядку маркерів кінця рядка.

Метод знаків однакової форми передбачає заміну літер українського (або російського) алфавіту на символи латинського, що мають однакове накреслення, проте різні коди символів. Метод має набагато більшу ємність по відношенню до методів, розглянутих вище. Однакове накреслення мають літери «a, c, e, i, o, p, x, y, A, B, C, E, H, I, K, M, O, P, T, X», причому літери «a, e, c, i, o» належать до таких, що найбільш імовірно з'являються (мають максимальну частоту) у текстах української мови. До того ж кількість бажаних літер можна збільшити навмисно, підібравши відповідний текст.

Додатково можна говорити про різні символи для дефісів, різні варіанти пробілів (наприклад, пробіл у стилі *italic*) та інші, проте при цьому слід проводити додаткові дослідження щодо підтримки символів редакторами та засобами відображення візуальної частини ресурсу з клієнтського боку. Якщо мова не іде про символи пробілу, то інші символи мають значно меншу частоту появи і у порівнянні з літерами матимуть незначну стеганографічну ємність.

Для підвищення ступеня захисту інформаційних ресурсів варто періодично змінювати зміст стеганографічного повідомлення. Якщо зловмисник намагається створити клон інформаційного ресурсу, то наповнення клієнтської частини він просто скопіює з оригінального ресурсу. Очевидно, що копія міститиме всі стеганографічні елементи, які були в оригіналі, навіть якщо зловмисник не підозрює про їх наявність.

Пропонується використання дати і часу як змісту стеганографічної інформації. Оновлювати інформацію варто щоразу, коли надходить запит серверу до даного інформаційного ресурсу. Відповідний режим внесення змінної інформації слід вважати динамічною стеганографією.

Модуль перевірки автентичності інформаційного ресурсу може встановлюватися на клієнтському боці і перевіряти збіг значення часу, який передається сервером у складі протоколу обміну, та часу, який визначається з прихованого стеганографічного повідомлення.

З метою покращення надійності захисту можна використовувати додаткове криптографічне перетворення дати і часу з використанням разових ключів, обмін якими може відбуватися між інформаційним ресурсом та модулем перевірки автентичності до завантаження візуальної частини ресурсу.

ВИСНОВКИ

Наведено порівняльний аналіз методів комп'ютерної стеганографії при застосуванні для задач захисту інформаційних ресурсів. Показано недоліки використання статичних зображень як стегоконтейнерів. Запропоновано впровадження методів динамічної стеганографії з вибором текстових стегоконтейнерів за принципом цифрових «водяних» знаків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] **Барсуков, В. С.** Компьютерная стеганография вчера, сегодня, завтра [Текст] / В. С. Барсуков, А. П. Романцов. – М. : Специальная техника, 1999. – 432 с.

[2] **Конахович, Г. Ф.** Компьютерная стеганография. Теория и практика [Текст] / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

Надійшла до редколегії 14.02.13
Статтю рекомендує до друку член редколегії Вісника НУК
д-р техн. наук, проф. *В. С. Блінцов*
Статтю розміщено у Віснику НУК № 1, 2013