УДК 004.056

ЗАХИСТ ІНФОРМАЦІЇ ЗАСОБАМИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Іванов Володимир Георгийович

доктор технічних наук, професор,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: vladimir-ivanov33@rambler.ru
ORCID: 0000-0001-5619-2839

Забезпечення надійного захисту інформації від несанкціонованого доступу є однією з якнайдавніших проблем, яка, на жаль, не вирішена й до теперішнього часу. Зазначимо, що усунути її можна лише за допомогою методів стеганографії [1; 2]. Стеганографія (від грец. Steganos – таємниця, секрет і грец. Graphy – пишу; буквально «тайнопис», секретний лист) – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту існування секретного повідомлення. Стеганографія застосовується для захисту інформації, а її історія налічує тисячоліття. Відомі факти використання голови людини, у якої під волоссям знаходилося секретне повідомлення, що перед цим їй нанесли на поголений череп. У стеганографії вживають sympathetic ink (невидимі) чорнила. Текст, записаний таким чорнилом, проявляється тільки за певних умов (нагрів, освітлення, хімічний проявник та ін.). Під час Другої світової війни активно використовувалися мікроточки – мікроскопічні фотознімки, які вклеюються в текст листів, телеграм.

Нині існує і розвивається комп'ютерна стеганографія (КС), предметом вивчення якої є методи, що приховують інформацію в потоках оцифрованих сигналів із використанням комп'ютерної техніки та програмного забезпечення. Цей новий напрямок наукових досліджень поєднує в собі

останні досягнення криптографії, теорії інформації, торії ймовірностей і математичної статистики, цифрової обробки сигналів і зображень, теорії дискретних Фур’є і вейвлет – перетворень, кодування і стиснення даних. Завдання КС – захистити інформацію від несанкціонованого використання за допомогою розміщення (вбудовування) одних даних (секретних повідомлень) в інші (контейнер) таким чином, щоб візуальний або технологічний доступ до повідомлень був неможливий. Розрізняють контейнери двох типів. Контейнер-оригінал (або "порожній" контейнер) – це контейнер, який не містить прихованих повідомлень. Контейнер – результат (або "заповнений" контейнер, стеганоконтейнер) – це контейнер, який містить приховані повідомлення. Порожній і заповнений контейнери не повинні відрізнятися один від одного [5].

Стеганографічна система (стеганосистема) являє собою сукупність порожніх контейнерів, повідомлень, ключів, заповнених контейнерів і перетворень, які їх пов'язують (алгоритмів впровадження та вилучення). Як порожні контейнери можуть використовуватися комп’ютерні файли, цифрові зображення, звук, відео, а як секретне повідомлення – будь-який текст або чорно-біле зображення, наприклад, креслення або схема. Під ключем розуміються секретні дані, які визначають порядок занесення повідомлення в контейнер.

Базові вимоги до стеганосистем: 1) невідчутність: впровадження повідомлення повинно зберегти якість вихідного порожнього контейнера; для аудіосигналів повідомлення має бути нечутним, для зображень – візуально непомітним; 2) стійкість (безпека): несанкціонований користувач не повинен мати можливість відрізнити заповнений контейнер від порожнього, використовуючи методи візуального або статистичного аналізу, а також цілеспрямованих атак на повідомлення; 3) пропускна здатність (або місткість): визначається як максимальна кількість даних повідомлення, яке може бути впроваджене в контейнер з дотриманням вимог невідчутності і стійкості; 4) обчислювальна складність: впровадження і витяг повідомлення

має відбуватися досить швидко, щоб задовольняти вимоги додатків реального часу (наприклад, потокове аудіо або відео).

Існують два основні методи комп'ютерної стеганографії: 1) методи, засновані на використанні спеціальних властивостей комп'ютерних форматів; 2) методи цифрової обробки сигналів, засновані на надмірності аудіо- і візуальної інформації. Перший напрям передбачає застосування спеціальних властивостей комп'ютерних форматів представлення даних. Спеціальні властивості форматів обираються з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або прочитання (наприклад, вільний кластерний простір файлів, частина поля розширень, що не заповнена інформацією та ін.). Недоліком цих методів є низький ступінь прихованості і малий обсяг переданої інформації. Основним напрямом комп'ютерної стеганографії виступає використання надмірності аудіо- і візуальної інформації. У цьому випадку широко застосовується метод заміни найменшого значущого біта (НЗБ. LSB - Least Significant Bit). Можливість такої заміни пояснюється наявністю в зображенні структурної і психофізичної надмірності. Цифрове зображення і цифровий звук – це числа, які представляють собою інтенсивність світла або звукового сигналу в моменти часу, що йдуть послідовно. Усі ці числа не точні, оскільки не точні пристрої оцифрування аналогових сигналів, є шуми квантування. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку і візуального образу. Їх заповнення відчутно не впливає на якість сприйняття, що і дає можливість для приховування додаткової інформації. Зміна кожного з трьох найменших значущих біт графічного кольорового зображення приводить до зміни менше 1% інтенсивності даної точки, що дозволяє приховувати в стандартній графічній картинці об'ємом 800 Кбайт близько 100 Кбайт інформації, непомітної при перегляді зображення. Одна секунда оцифрованого звуку у стерео-режимі дозволяє приховати за рахунок заміни найменших значущих молодших розрядів близько 10 Кбайт інформації.

Вбудовування повідомлення в цифровий контейнер (зображення або аудіофайл) може проводитися за допомогою ключа, одного або декількох. Ключ – спеціальні вихідні дані, які запускають роботу генератора випадкових чисел (ГВЧ) за відповідним алгоритмом. Числа, что породжуються генератором ГВЧ, можуть визначати позиції відліків, які модифікуються, у разі фіксованого контейнера або інтервалів між ними у разі потокового контейнера. Ключі повинні бути відомі партнерам по зв'язку. Заміна НЗБ може здійснюватися так само у спектральних коефіцієнтах різних ортогональних перетворень (Косинусному, Хаара, Фур'є та ін.) вихідного повідомлення [3; 4].

Виділяють наступні стеганосистеми: 1) системи прихованої передачі або зберігання даних для організації прихованої комунікації; 2) цифрових водяних знаків (ЦВЗ-невеликі текстові та числові дані); мають таке практичне застосування, як: контроль цілісності знімків камер відеоспостережень, записів телефонних розмов, фотознімків, які використовуються як докази в суді, аутентифікація власника даних (захист авторських прав і прав власності); 3) ідентифікаційних номерів – унікальні ЦВЗ, які впроваджуються в набір цифрових копій контейнера для їх подальшої ідентифікації і контролю поширення; 4) системи заголовків для прихованої анотації медичних знімків, швидкий пошук в мультимедійних базах даних та ін.

Методи комп'ютерної стеганографії стають у нагоді і при реалізації злочинних цілей для планування і приховування злочинів. Виявлення факту приховування повідомлень (стеганоаналіз) – одне з найбільш актуальних і складних завдань комп'ютерної стеганографії. Серед методів практичного стеганоаналізу розрізняють візуальну і статистичну атаки. Ці атаки запропоновані для виявлення факту впровадження прихованої інформації в молодші розряди елементів контейнера. При цьому на виході стеганосистеми відмінність між контейнером і стеганоконтейнером візуально не виявляється. Однак якщо стеганоконтейнер сформований тільки з НЗБ пікселів, то можна

побачити сліди вкладення у вигляді ділянки хаотичного шуму. НЗБ порожнього контейнера шуму не дають і не дозволяють візуально визначити зміст (сліди) вихідного зображення. Більш ефективними вважаються атаки, які базуються на відмінних статистичних характеристиках порожніх і заповнених контейнерів. Статистичні методи стеганоаналізу використовують як характеристики оцінки ентропії, коефіцієнти кореляції, умовні розподіли та ін. Ступінь відмінності між цими характеристиками визначає ймовірність існування стеганографічного каналу. Легітимний стеганоаналіз має можливості виявлення стеганографічного каналу, вилучення, руйнування і підміни прихованого повідомлення. Несанкціонований стеганоаналіз володіє тими ж можливостями (загрозами), що і легітимний.

Список використаної літератури

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В.Туринцев. – М. : СОЛОН-Пресс, 2002. – 261 с.

2. Інтеграція права й інформатики: прикладний та змістовний аспекти / за заг. ред.: В. Г. Іванов, В. Ю. Шепітько. – Харків : Право, 2012. – 250 с.

3. Иванов В. Г. Фурье и вейвлет-анализ изображений в плоскости JPEG технологий / В. Г. Иванов, М. Г. Любарский, Ю. В. Ломоносов // Проблемы управления и информатики. – 2004. – № 5. – С. 111–124.

4. Кошкина Н. В. Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы / Н. В. Кошкина // Проблемы управления и информатики. – 2010. – № 5. – С. 132–144.

5. Хорошко В. А. Введение в компьютерную стеганографию / В. А. Хорошко, М. Е. Шелест. – Киев : НАУ, 2002. – 140 с.