АНАЛІЗ КРИТЕРІЇВ ЕФЕКТИВНОСТІ ГРАФІЧНИХ СТЕГАНОСИСТЕМ

Піліпіха О. В.
Кухарська Н. П., к. ф.-м. н., доцент
Львівський державний університет безпеки життєдіяльності

На даний час більшість досліджень у сфері стеганографії базується на використанні цифрових зображень як стеганоконтейнерів. До цього, як вважають автори [1], призвела ціла низка причин.

Способів стеганографічного приховування секретних повідомлень у графічних файлах на сьогодні відомо доволі багато, однак проблема вибору відповідного контейнера до сих пір не вирішена. А від цього залежить стійкість заповненого стегоконтейнера до різних видів аналізу: візуального, статистичного.

Під терміном «ефективність» будемо розуміти здатність стеганосистеми вирішувати основні завдання стеганографії: швидко і приховано передавати великі обсяги секретної інформації. Існує дуже велика кількість факторів, вплив яких позначається на ефективності побудованих стеганосистем. Серед них можна виокремити групу технічних критеріїв, які піддаються строгому математичному описові і мають певний набір кількісних характеристик. Існують й інші критерії, так звані, якісні, які не можливо описати через математичні формули, але, які відіграють не менш важливу роль у формуванні поняття «ефективність». Проаналізуємо їх.

Невидимість (стеганографічна стійкість). Задоволення вимоги невидимості є обов'язковим для всіх без винятку стеганосистем. Що стосується графічної стеганосистеми, то тут стійкість пов'язана зі змінами (спотвореннями), що вносяться у вихідне зображення при вбудовуванні повідомлення. Вимога стійкості вважається невиконаною, якщо зображення піддається атаці звичайного візуального аналізу.

Пропускна здатність. Ефективність використання цифрового зображення для зберігання секретної інформації в значній мірі залежить від того, яку максимальну кількість байт повідомлення можна в нього помістити. Чисельно цей критерій, як правило, визначається як процентне співвідношення між обсягом вбудованого повідомлення й обсягом контейнера. Своєрідним «обмежувачем» максимального розміру повідомлення для графічного файлу фіксованого розміру виступає описана вище вимога невидимості. Встановлена фундаментальна залежність між стеганографічною стійкістю та розміром повідомлення. Ця залежність має обернено пропорційний характер: чим більший об'єм повідомлення, вбудованого в заздалегідь обраний контейнер, тим нижча надійність його приховування.

Стійкість до модифікацій заповненого контейнера (стиснення) характеризується ймовірністю відновлення повідомлення за умови, що заповнений контейнер зазнав деякої модифікації. Окремим випадком модифікації є стиснення з втратами. Особливе значення цей чинник ефективності має для технології впровадження цифрових водяних знаків (ЦВЗ). Модифікація заповненого контейнера може здійснюватися як ненавмисно (стиснення, помилки при передачі файлу каналами зв'язку з завадами), так і навмисно (через спроби порушити авторські права шляхом знищення ЦВЗ).

Обсяг обчислень, необхідний для вбудовування повідомлення в цифрове зображення. Незважаючи на стрімке зростання потужності сучасних комп'ютерів, проблема обчислювальної складності алгоритмів вбудовування продовжує відігравати ключову роль у деяких випадках застосування стеганографії. Це, як правило, інформаційні системи реального часу, де часові рамки виконання алгоритму є обмежені. Як приклад, можна навести прихований канал голосового зв'язку: аудіоінформація вбудовується в потік графічних файлів, що передаються мережею. Очевидно, що в даному випадку, щоб уникнути втрати якості переданої інформації, пакети даних (цифрові зображення) повинні заповнюватися повідомленнями і доставлятися миттєво.

Використовуваний графічний формат. Значною мірою ефективність застосування цифрових зображень в стеганографії залежить від формату їх зберігання. У комп'ютерній графічній стеганографії найбільш поширеним типом носія є файли зображення формату BMP. Це пояснюється тим, що для цілей стеганографії найбільш придатними є файли форматів, в яких використовуються методи стиснення без втрат (такі види стиснення типові для зображень формату BMP, TIFF, PNG, TGA, й ін.). Також аргументом на користь вибору формату BMP виступає висока якість зображення і простота формату.

ЛІТЕРАТУРА

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