

СТЕНОГРАФІЧНІ МЕТОДИ ЯК ЗАСІБ БОРОТЬБИ З НЕСАНКЦІОНОВАНИМ ДОСТУПОМ

Дуже часто при зберіганні та передачі інформації, а особливо економічної або фінансової інформації, виникає потреба у її приховуванні від сторонніх очей. Тому вусьому світі назріло питання розробки методів (засобів) захисту інформації організаційного, методологічного й технічного характеру, серед них – методи криптографії та стеганографії.

Для гарантованого захисту вмісту повідомлення існує два різних підходи [1-2]: блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення; повідомлення, яке передається, намагаються приховати так, аби його неможливо було знайти. За першим підходом використовують криптографічні методи захисту. Другий підхід застосовує стеганографічні методи захисту. На відміну від криптографічного захисту, стеганографічні методи дозволяють вмонтувати інформацію, що передається, в невинні послання так, щоб не можна було навіть запідозрити існування підтексту. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Інтерес до стеганографії відродився в останнє десятиліття і був викликаний широким поширенням технологій мультимедіа, що пов'язані із захистом інформації. Ще в 1883 р. фламандський криптограф А. Керхгофс (А. Kerckhoffs) указував на той факт, що система захисту інформації повинна виконувати покладені на неї функції навіть при повній інформованості противника про її структуру та алгоритм функціонування [3]. Вся таємність системи захисту переданих повідомлень повинна втримуватися в ключі – фрагменті інформації, попередньо, як правило, розділеному між адресатами.

Цифрова стеганографія як містить у собі такі напрями: вбудовування інформації з метою її прихованої передачі; вбудовування цифрових водяних знаків (ЦВЗ) (watermarking); вбудовування ідентифікаційних номерів (fingerprinting); вбудовування заголовків (captioning).

ЦВЗ можуть застосовуватися, в основному, для захисту відкопіювання та несанкціонованого використання. Прикладами можуть бути фотографії, аудіо- та відеозаписи та ін. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в захисті об'єкта невидимих міток – ЦВЗ.

Технологія вбудовування ідентифікаційних номерів виробників

має багато загального з технологією ЦВЗ. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний вбудований номер (звідси й назва – дослівно "відбитки пальців"). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища.

Одна із найбільш розвинених на сьогоднішній день група методів вбудовування інформації з метою її прихованої передачі – заміна найменш значущого біта (LSB – LeastSignificantBit) в просторовій множині [3]. Молодший значущий біт зображення несе в собі найменше інформації. Відомо, що людина в більшості випадків не здатна помітити змін у цьому біті. При цьому для зображення в градаціях сірого обсяг убудованих даних може становити 1/8 від загального обсягу контейнера. Популярність цього методу обумовлена його простотою й тим, що він дозволяє приховувати у відносно невеликих файлах досить великі обсяги інформації. Метод найчастіше працює з растровими зображеннями, представленими у форматі без компресії (наприклад: GIF і BMP). Недоліком методу LSB є чутливість до розміру зображення, тобто чим менший розмір зображення, тим більше будуть відрізнятися два сусідні пікселі, тому пропонується використовувати зображення з великою роздільністю. Попри це, метод запису LSB є досить популярним, стійким та простим в реалізації. Існує багато модифікацій цього методу запису, кожна з яких дозволяє корегувати стенографічні процеси в залежності від потреб.

Підводячи підсумок, можна сказати, що використання стенографічного методу LSB для усунення несанкціонованого доступу до даних є ефективним та активно запровадженим рішенням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Барсуков В.С., Романцов А.П. Комп'ютерна стеганографія вчора, сьогодні, завтра [Електронний ресурс]. – Режим доступу: <http://www.bnti.ru/showart.asp?aid=330&lvl=03.07.06> (дата звернення 03.03.2020). – Назва з екрана.
2. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика [Текст] Г.Ф.Конаховіч, А.Ю. Пузиренко. – К.: МК-Пресс, 2006. – 288 с.
3. Kerckhoffs A. LaCryptographicMilitaire / A. Kerckhoffs/[Journaldessciencesmilitaire]. – 1983. – Jan. – P. 5 – 83; 1983. – Feb. – P. 161–191.