СТЕГАНОГРАФІЧНИЙ ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ МЕТОДОМ КУТТЕРА-ДЖОРДАНА-БОССЕНА

Наталія Кухарська, Дмитро Прокопечко

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The problem of information security through its steganographic hiding in a graphics container. Improving the method of Kutter-Jordan-Bossen that performs steganographic implementation of spatial data in raster image area. The improvement is the introduction of a method of additional rules that eliminate the problem of retrieval. The research results improved method in developed among its implementation.

Keywords: steganography, data hiding, data protection, introduction of data, spatial region.

У зв'язку з бурхливим розвитком комп'ютерних технологій і активним проникненням їх у всі сфери людського буття однією з актуальних проблем на сьогодні є проблема захисту інформації.

Стеганографія як самостійна теоретично-прикладна наука дає змогу вирішувати такі важливі завдання інформаційної безпеки як захист авторських прав на мультимедійні дані від піратства за допомогою використання, так званих, цифрових водяних знаків, а також захисту конфіденційної інформації від ознайомлення сторонніх осіб під час обміну нею шляхом організації скритого каналу передачі даних.

На відміну від криптографії, що приховує вміст секретного повідомлення, стеганографія приховує сам факт його наявності. Таким чином, під поняттям приховання існування інформації з точки зору стеганографії розуміється не тільки неможливість виявлення в перехопленому повідомленні схованих даних, але й взагалі унеможливлення виникнення будь-яких підозр з цього приводу.

Шифрування конфіденційної інформації проблему неавторизованого доступу до неї повністю не вирішує, так як наявність зашифрованого повідомлення вже саме по собі привертає увагу «супротивника». Перехопивши криптографічно захищений файл, він неодмінно зацікавиться ним й докладе максимум зусиль, щоб розшифрувати його. У зв’язку з цим, для передачі секретної інформації незахищеними каналами зв’язку сьогодні активно використовують також стеганографічні методи. Стеганографія не замінює, а доповнює криптографію. Приховання повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі конфіденційного повідомлення, а якщо приховане повідомлення до того ж зашифроване, то воно матиме ще один, додатковий, рівень захисту.

Загальною рисою стеганографічних методів є те, що приховуване повідомлення вбудовується в інформаційно непримітний об'єкт (контейнер), який згодом відкрито пересилається адресатові.

Найбільш перспективним напрямком стеганографії на сьогоднішній день є цифрова стеганографія – напрямок комп'ютерної стеганографії, заснований на прихованні інформації в цифрових об'єктах, що початково мають аналогову природу (зображення, відео, звук). У зв'язку з розвитком апаратних засобів обчислювальної техніки й величезною кількістю каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості представлення інформації у файлах, обчислювальних мережах і т. п.

Метою роботи є розроблення комп’ютерних програм вбудовування/видобування секретної інформації для її зберіганні або передачі відкритими каналами зв'язку й дослідження стійкості побудованої стеганосистеми залежно від кількості прихованої інформації й особливостей самого процесу вбудовування.

Згідно алгоритму методу Куттера-Джордана-Боссена (КДБ) [5] конфіденційна інформація вбудовується в канал синього кольору зображення, що має RGB-кодування. Канал саме цього кольору обраний авторами не випадково, а виходячи з тих міркувань, що зорова система людини є найменш чутливою до змін внесених в синю складову.

Алгоритм методу КДБ ґрунтується на використанні методів екстраполяції (прогнозування) випадкових сигналів.

Екстраполяція – це метод, згідно якого результати отримані із спостережень над однією частиною деякого явища поширюються на його іншу частину. У більш вузькому сенсі – це визначення за рядом даних функції інших її значень поза цим рядом. У процесі видобування секретного біту, отримувачу необхідно передбачити початкове значення немодифікованого пікселя на основі значення декількох сусідніх пікселів, що розташовані у тому ж рядку і в тому ж стовпці заповненого стеганоконтейнера. Автори методу використовують "хрест" розміром 7х7 пікселів.

Перед вилученням повідомлення з стеганоконтейнера повинні бути відомі:

- заповнений контейнер;
- первинний ключ;
- кількість циклів обчислення координат;
- кількість дублюючих вбудовувань одного біта;
- розмір хреста – кількість пікселів зверху (знизу, зліва, справа) від оцінюваного пікселя.

У роботі використано удосконалення методу КДБ, запропоновані у [2]. Вони полягають у введенні в алгоритм методу додаткових правил, метою яких є усунення проблем видобування даних, що пов'язані з окремими випадками заповнення вихідного контейнера.

За рахунок модифікацій були усунені помилки видобування:

- секретних бітів з одиничним значенням з областей контейнера, в яких пікселі мають максимальне значення по синьому каналу;
- секретних бітів з нульовим значенням з областей контейнера, в яких пікселі мають мінімальне (нульове) значення по синьому каналу;
- секретних бітів з одиничним значенням з областей контейнера, в яких всі пікселі мають чорний колір;
- секретних бітів з областей контейнера, в яких містяться дрібні деталі, що сильно відрізняються за кольором від фону.

Досліджено, що метод стійкий до багатьох відомих видів атак: низькочастотної фільтрації зображення, його компресії, обрізання країв, розмивання.

Розроблені в середовищі Mathcad на основі використання методу КДБ програми можуть бути використані для вбудовування секретних даних у зображення з метою передавання їх загальнодоступними відкритими телекомунікаційними каналами.

Література

1. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М. : Солон- Пресс, 2009 – 272 с.
2. Защелкин К.В. Усовершенствование метода стеганографического скрытия данных Куттера-Джордана-Боссена / Защелкин К.В., Иващенко А.И., Иванова Е.Н. // Радіоелектронні і комп'ютерні системи. – 2013. – № 5. – С. 151-155.
3. Конахович Г.В. Компьютерная стеганография. Теория и практика / Конахович Г.В., Пузыренко А.Ю. – К. : "МК- Пресс"», 2006. – 288 с.
4. Кузнецов О.О. Методи обробки сигналів даних та зображень : навч. посібник / Кузнецов О.О., Кучук Г.А., Семенов С.Г. –.Харків : НТУ "ХПІ", 2011. – 310 с.
5. Kutter M. Digital Signature of Color Images using Amplitude Modulation / Kutter M., Jordan F., Bossen F. // Proc. SPIE Storage and Retrieval for Image and Video Databases. – 1997. – Vol. 3022. – P. 518-526.