УДК 004.056.5

М. В. Мигидин

ВДОСКОНАЛЕННЯ СТЕГАНОГРАФІЧНОГО МЕТОДУ КУТТЕРА-ДЖОРДЕНА-БОССЕНА В РАСТРОВИХ ЗОБРАЖЕННЯХ ЗА РАХУНОК ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ

Вінницький національний технічний університет

Анотація

Запропоновано вдосконалення методу Куттера-Джордана-Боссена, що виконує стеганографічні приховування даних в просторовій області растрового зображення. Вдосконалення полягає у введенні в метод додаткових правил, що усувають проблеми вилучення даних і підвищують пропускну здатність методу.

Ключові слова: інформація, захист інформації, приховування даних, стеганографія.

Abstract

The report improving the Cutter-Jordan-Bossen steganographic method, which performs steganographic hiding data in a spatial region of bitmap. The essence of perfection is the introduction in the method additional rules, which can eliminate the problem of the data extraction and increases throughput of the method.

Keywords: information, information security, data hiding, steganography, method.

Вступ

Завдання захисту інформації від несанкціонованого доступу є однією з найстаріших завдань, що вирішуються людством. Одними з найефективніших методів приховування інформації є стеганографічні методи. Основна задача стеганографії – приховати секретне повідомлення та передати його отримувачу так, щоб приховати факт передачі повідомлення. Найчастіше у системах безпеки в якості контейнерів для повідомлень використовуються растрові зображення. При приховуванні повідомлення слід використовувати такі методи, які внесуть мінімальний вплив на контейнер, тобто після вбудовування повідомлення, контейнер не викличе підозри у зловмисника. Стегосистема складається із стегоконтейнера, секретного ключа, секретного повідомлення, оригінального файлу. Існуючі системи поділяються на ті, що вимагають наявності первісного зображення, що робить передачу незручною, а також ті, що вимагають знання секретного ключа для вилучення повідомлення. Системи першого типу вносять незначні зміни у стегоконтейнер, але виникає складність передачі повідомлення через необхідність наявності у отримувача первісного зображення. Системи другого типу вимагають знання секретного ключа для вилучення повідомлення. Такі системи є найбільш зручними для передавання секретних повідомлень.

Сьогодні постала необхідність вбудовування більшого об`єму інформації у растрові зображення і постає питання необхідності підвищення пропускної здатності методу приховуваннях інформації в растрових зображеннях, тож обрана тема є актуальною на сьогоднішній день. Зараз існує потреба в приховуванні все більшого об’єму інформації, тому проблема захисту інформації від несанкціонованого доступу стає все більш актуальною в даний час. На ряду з криптографічними методами захисту існують стеганографічні методи, які на відміну від криптографії приховують сам факт існування прихованих даних. Стеганографічні алгоритми широко застосовуються для вирішення наступних завдань: захисту конфіденційної (службової) інформації від несанкціонованого доступу, захисту авторського права на інтелектуальну власність, подолання систем моніторингу і управління мережевими ресурсами, камуфлювання програмного забезпечення, створення прихованих каналів витоку інформації [1].

Найбільшої популярності здобули методи (алгоритми) приховання інформації, що використовують у якості контейнера зображення. Це обумовлено наступними причинами: відносно великим об’ємом представлення зображень, високою пропускною здатністю, відсутністю обмежень, що накладаються вимогами реального часу, слабкою чутливістю людського зору до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів, необхідністю захисту від незаконного розповсюдження [2]. Існує багато різноманітних стеганографічних методів, але кількість інформації, яку можна вбудувати обмежена. При збільшенні пропускної здатності автоматично погіршується якість зображення та стійкість до атак, якщо підвищувати стій-

кість до атак – зменшиться пропускна здатність і погіршиться якість зображення. Під пропускною здатністю приховуваних даних розуміють максимальну кількість інформації, яка може бути вбудована до одного елементу (наприклад, пікселя) контейнера, обов'язковою умовою при цьому є безпомилковість передачі приховуваних даних одержувачеві, а також їх захищеність від атак порушника [4].

Більшість існуючих методів вбудовують інформацію в просторову область зображення, але вони досить нестійкі до навмисних та ненавмисних атак. Тому доцільно використовувати методи приховування інформації в частотну область зображення, які стійкіші до атак, проте їхнім недоліком буде гірша пропускна здатність. Ідея методу Куттера-Джордана-Боссена базується на особливості зорової системи людини, а саме на найменшій чутливості людського ока до синього кольору в моделі RGB. Даний метод відрізняється високою стійкістю до активних стеганографічніх атак стисненням, геометричним перетворенням і розмиванням [3]. Таким чином задача вдосконалення даного стеганографічного методу приховування інформації, а саме підвищення пропускної здатності і збереження стійкості до атак є актуальною та важливою сьогодні.

Результати дослідження

В доповіді проведене дослідження практичної реалізації методу Куттера-Джордана-Боссена, проаналізовано ряд проблем, пов'язаних з характером зображення, що зберігається в вихідному стегоконтейнері [5]. Проблеми вбудовування, і відповідно вилучення, секретних даних при наявності у вихідному контейнері областей, в яких більшість пікселів мають: максимальне значення по синьому каналу, нульове значення по синьому каналу, чорний колір (мінімальне значення за всіма кольоровими каналами).

За запропонованими модифікаціями [6-7] методу Куттера-Джордана-Боссена були проведені експериментальні дослідження. Вихідним матеріалом для експериментів були растрові зображення, що розрізняються за походженням (фотознімки та синтетичні зображення), розміром, різними частинами областей суцільного одного кольору і областей, що містять дрібні контрастні деталі. Проведені експерименти показали, що запропоновані модифікації методу дозволяють правильно витягувати секретні повідомлення з фрагментів зображень-контейнерів, на яких традиційний метод давав помилку вилучення, а також усунути помилки вилучення 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 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 дуже дрібні деталі, а також підвищення стійкості та пропускної здатності методу.

Робота присвячена вирішенню актуальної проблеми підвищення пропускної здатності методу приховування інформації у растрових зображеннях.

Вдосконалення полягає у вбудовуванні даних у 2 канали, що повинно підвищити пропускну здатність методу та використанні іншої колірної моделі для зменшення помітності вбудовування. В якості стегоконтейнерів було запропоновано використовувати файли формату JPEG. Метод підвищення пропускної здатності реалізовано за рахунок використання не лише синього каналу, а й червоного, завдяки цьому розмір вбудовуваного повідомлення було збільшено майже вдвічі. Але погіршилась якість зображення, тому для зменшення помітності змін у зображенні було використано іншу колірну модель, а саме колірну модель YCbCr.

Стійкість як існуючого методу, так і вдосконаленого є досить високою, оскільки виконується дотримання головної вимоги стеганографії – непомітності передавання інформації. Проведений експеримент показав, що вбудовування інформації є найбільш ефективним у 2 канали з використанням перетворення у колірну модель YCbCr.

Також було виконано реалізацію програмного додатку на основі вдосконаленого методу, а саме розроблено програму для вбудовування інформації у зображення. В програмі реалізовано функціонал до кожного з модулів, а саме: вибір зображення, вибір текстового файлу для вбудовування та вилучення прихованої інформації. Було виконано проектування зручного інтерфейсу користувача, який не викликає складності при роботі з програмою.

Висновки

Проаналізовано існуючі стеганографічні методи приховування інформації в растрових зображеннях. Удосконалено стеганографічний метод Куттера-Джордана-Боссена, а саме підвищено пропускну

здатність методу приховування інформації в растрових зображеннях, збергіючи при цьому стійкість до атак. Розроблено алгоритм та програмний засіб для реалізації вдосконаленого методу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конахович Г.Ф. Комп'ютерна стеганографія / Г.Ф. Конахович, А.Ю. Пузиренко. – К.: МК-Пресс, 2006. – 288 с.
2. Грибунін В.Г. Цифровая стеганография / В.Г. Грибунін. – М.: Салон-прес, 2002. – 344 с.
3. Аграновський А.В. Основи комп'ютерной стеганографії / Аграновський А.В., Девянін П.Н., Р.А. Хаді, Черемушкін А.В. – М.: Радіо та зв'язок, 2003. – 152 с.
4. V. Karpinets, Ju. Yaremchuk, M. Prokofjev. Матеріали конференції, Technical University of Gabrovo. International scientific conference UNITECH'12. / V. Karpinets, Ju. Yaremchuk, M. Prokofjev. // Proceedings. Volume I, 16–17 November 2012, Gabrovo. – Pp. 348 – 352.
5. Kutter, M. Digital Signature of Color Images using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc. SPIE Storage and Retrieval for Image and Video Databases. – 1997. – Vol. 3022. – P. 518-526.
6. Михайличенко О.В. Підвищення стійкості стеганоалгоритмів частотної області на основі дискретно-косинусного перетворення до зовнішнього впливу // Михайличенко О.В., Прохожев Н.Н., Коробейников А.Г. Науково-технічний вісник СПб ГУ ІТМО – СПб.: СПб ГУ ІТМО, 2009.– вип. 2(60). – С.102 – 104.
7. Защелкін К.В., Іващенко А.І., Іванова Е.Н. Вдосконалення методу приховування даних Куттера-Джордана-Боссена/ Защелкін К.В., Іващенко А.І., Іванова Е.Н.- Одеса: ОНТІ, 2013 - 151с.

Марина Вікторівна Мигидин – студентка групи УБ-12, факультет менеджменту, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: marinka.dir@gmail.com.

Науковий керівник: ***Василь Васильович Карпінець*** – канд.техн.наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Maryna V. Myhydyn – student of group UB-12, Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Vasyl V Karpinets*** – Cand. Sci. (Eng.), Docent of Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.