УДК 004.056.5

Г. А. Дмитрук
В. В. Карпінець

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЯК ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС КОНФІДЕНЦІЙНОГО СПІВРОБІТНИЦТВА

Вінницький національний технічний університет

Анотація

Проаналізовано стеганографічні методи захисту інформації, їх доцільність та надійність використання під час обміну інформацією в конфіденційному співробітництві. Запропоновано використання найбільш надійного методу обміну даними між конфідентами.

Ключові слова: цифрова стеганографія, цифрові водяні знаки, контейнер, вбудоване (приховане) повідомлення, конфідент.

Abstract

Steganographic methods of information protection, their expediency and reliability of use in the exchange of information in confidential cooperation are analyzed. It is suggested to use the most reliable method of communication between confidential persons.

Keywords: digital steganography, digital watermarks, container, embedded (hidden) message, confidential.

Дослідження методів стеганографії невпинно зростає, адже з поширенням персональних комп'ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу великої кількості людей [1]. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних [2].

Найбільшої популярності здобули методи приховання інформації, що використовують у якості контейнера зображення. Це обумовлено наступними причинами: відносно великим об'ємом цифрового представлення зображень; відсутністю обмежень, що накладаються вимогами реального часу; наявністю в більшості реальних зображень областей текстур, що мають шумову структуру і відповідають вбудовуванню інформації [3].

Після дослідження та порівняльного аналізу стеганографічних методів для подальшого використання було обрано метод за особливими точками, які також називають семантичними методами або на основі вмісту, оскільки використовують оригінальні дані контейнера і не вносять в нього додаткових даних для синхронізації [4]. Відсутність додаткових шумів робить їх застосування непомітним порушнику, крім того ці методи стійкі до узагальнених і локальних геометричних спотворень, дозволяють паралельно із синхронізацією ідентифікувати області не придатні для вкраплення (гладкі) та можуть бути стійкими до JPEG стиснення, а також будь-яких спроб видалити частину інформації при збереженні перцепційної якості зображення [5].

Існуючі методи синхронізації ЦВЗ в контейнері-зображенні мать один суттєвий недолік, а саме невисоку стійкість до геометричних перетворень. Найбільше переваг мають методи синхронізації на базі особливих точок. Ці методи принципово відрізняються від інших тим, що вони використовують оригінальні дані зображення і, як наслідок, створюють для кожного зображення свій унікальний набір точок [2].

Метод, який запропоновано, включає в себе автоматичну синхронізацію ЦВЗ за особливими точками зображення. На відміну від таких альтернативних методів синхронізації, як використання шаблонів чи піків автокореляції структурного ЦВЗ, які можливо видалити без зміни візуальної якості захищуваного контейнера-зображення , у даному методі локалізація ЦВЗ кодується за допомогою контенту зображення і ЦВЗ не може бути знищеним без суттєвого спотворення контенту. Ще одна перевага методів цього класу полягає у тому, що автоматична синхронізація ЦВЗ виконується без привнесення у зображення додаткових шумів.

Для визначення особливих точок метод використовує детектор Харріса [6]. В ході дослідження виявлено, що цей детектор визначає більш стабільні особливі точки у порівнянні з альтернативними варіантами – детектором кутів SUSAN (Smallest Univalue Segment Assimilating Nucleus) та детектором Archard-Rouquet . Серед переваг детектора Харріса можна виділити інваріантність до повороту та зсуву, часткову інваріантність до зміни яскравості [7].

Характериним для данного методу є оптимізація по двох напрямках:

– по-перше, було запропоновано для вбудовування не всі блоки, а ті які найбільш підходять;

– по-друге, в частотній області блока вибираються на два коефіцієнти ДКП, а три, що значно зменшує спотворення блока-контейнера [8].

За такими показниками як, максимальна відмінність, середня абсолютна відмінність, відношення «сигнал-шум», якість зображення, нормована взаємна кореляція було здійснено оцінювання точності розробленого методу .

Отже, для захищеного обміну інформацією між кофідентами було запропоновано вдосконалення методу визначення особливих точок зображення-контейнера шляхом встановлення оптимального значення коефіцієнтів функції відгуку зображення, а також розроблено алгоритм вбудовування ЦВЗ в зображення-контейнер, що є стійким до геометричних атак та алгоритм видобування прихованого ЦВЗ з зображення контейнера. Пропонується створити програмне забезпечення на основі вдосконаленого методу та розробленого алоритму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хорошко В.О. Комп'ютерна стеганографія: [навчальний посібник] / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. –Вінниця : ВНТУ, 2017. –155 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
3. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2013. – 152 с.
4. Карпінець В. В. Аналіз впливу цифрових водяних знаків на якість векторних зображень / В. В. Карпінець, Ю. Є. Яремчук // Сучасний захист інформації. — 2011. — № 1. — С. 72—82.
5. В.О.Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є.Яремчук. Основи комп'ютерної стеганографії. – Вінниця ВДТУ, 2003.
6. Грибунин В.Г, Оков И.Н., Туринцев И.В. Цифровая стеганография. - М.: СОЛОН-Пресс, 2012.
7. Михайличенко О.В., Прохожев Н.Н., Коробейников А.Г. Повышение устойчивости стегано алгоритмов частотной области на основе дискретно-косинусного преобразования к внешним воздействиям // Научно-технический вестник СПб ГУ ИТМО – СПб.: СПб ГУ ИТМО, 2009.– вып. 2(60). – С.102–104.
8. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 –«Менеджмент» та 6.170103 –«Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. –Вінниця: ВНТУ, 2013. –44 с.

Дмитрук Ганна Анатоліївна — студентка групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: anytka2227@ukr.net

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця

Dmitruk Hanna A. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, email : anytka2227@ukr.net

Supervisor: **Karpinets Vasyl V**.—Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia.