УДК 004.056.5:003.27

МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ ДЛЯ ГРАФІЧНИХ ФАЙЛІВ

Піскун Я.А.
Науковий керівник – к.т.н., доц. Рахліс Д.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. АПОТ, тел. (057) 702-13-26) e-mail: yaroslav.piskun@nure.ua, факс (096) 176-58-50

Analyze the existing methods of steganography for graphic files, add ways to improve the degree of stability of the methods.

Вступ. Стеганографія — це практика приховування інформації всередині іншої інформації. Це можна зробити, вставивши повідомлення в зображення, аудіофайл або інший тип медіа. Мета стеганографії полягає в тому, щоб приховати існування повідомлення, утруднюючи або унеможливлюючи його виявлення без знання конкретної техніки, яка використовується для його приховування. Загальні стеганографічні методи включають вставку найменшого біта та перетворення частотної області. Стеганографія може використовуватися для різних цілей, наприклад для захисту конфіденційної інформації від несанкціонованого доступу або прихованої передачі даних.[1]

Ще один стеганографічний прийом називається «маскування та фільтрація». Цей метод передбачає застосування фільтра до зображення, а потім налаштування параметрів фільтра для вбудовування повідомлення. Це можна зробити, регулюючи колірний баланс або контрастність зображення.[2]

Стеганографію також можна використовувати в цифровому світі. Наприклад, його можна використовувати, щоб приховати шкідливий код у, здавалося б, невинному файлі зображення, аудіофайлі чи інших типах медіа. Це відоме як «цифрова стеганографія» і може використовуватися для приховування зловмисного програмного забезпечення або іншого зловмисного коду, призначеного для викрадення конфіденційної інформації або контролю над комп'ютером.

Стеганографія також може бути використана для приховування повідомлень у мережевому трафіку. Це відоме як «стеганографія мережі» і може використовуватися для уникнення виявлення брандмауерів або систем виявлення вторгнень.

Зміст дослідження. Для покращення стеганографічних методів можна використовувати:

- Шифрування: можна використовувати алгоритми шифрування, щоб зашифрувати дані, перш ніж приховати їх на зображенні

обкладинки. Це ускладнить доступ зловмисника до прихованих даних, навіть якщо він зможе виявити їх наявність;

- систему керування ключами: можна використовувати систему керування ключами, щоб гарантувати, що лише авторизовані сторони мають доступ до прихованих даних. Це можна зробити за допомогою загального секретного ключа або системи публічно-приватного ключа;
- використовувати адаптивне вбудовування: можна використовувати адаптивні методи вбудовування, які регулюють процес вбудовування на основі характеристик зображення обкладинки. Це може зробити приховані дані більш непомітними, а тому їх буде важче виявити;
- використовувати контрзаходи стеганалізу: ви можете використовувати контрзаходи стеганалізу, щоб ускладнити зловмиснику виявлення прихованих даних. Це можна зробити за допомогою таких методів, як розширений спектр і рандомізація;
- використовувати передові методи такі як машинне навчання та нейронні мережі, щоб покращити ефективність методу стеганографії. Це може включати використання цих методів для розробки більш надійних і ефективних алгоритмів вбудовування або для розробки етодів стеганалізу, які є більш ефективними для виявлення прихованих даних;
- використовувати комбінацію різних методів для підвищення безпеки та ефективності методу стеганографії, наприклад, можна використовувати шифрування та адаптивне вбудовування разом.

Протестувати методи за допомогою стеганоаналізу, прослідкувати як змінилися результати тестування в залежності від покращення методу, оцінити якість програмного забезпечення [3].

Висновок. Наукова новизна полягає у дослідженнях методів комп'ютерної стеноганографії та покращення їх захисту до стеганоаналізу, непомітності та надійності проти обробки зображень.

Перелік джерел посилання:

1. . Marius Iulian Mihailescu, Stefania Loredana Nita, Cryptography and Cryptanalysis in MATLAB. 1st Ed (english), 2021.

2. Abbas Cheddad, Digital Image Steganography: Concepts, Algorithms, and Applications, 2009

3. Кучеренко Д.Е., Кривуля Г.Ф., Шкиль А.С.., Экспертное оценивание качества программного обеспечения, 2013.