УДК 621.375.4

О.Д.Азаров [1]
А.В. Гонца [2]
І.С. Колесник [3]

ЗАСІБ ДЛЯ ВБУДУВАННЯ ПОВІДОМЛЕННЯ У ФОТОГРАФІЇ ІЗ ЗБЕРЕЖЕННЯМ СТРУКТУРИ КОНТЕЙНЕРА

[1] Вінницький національний технічний університет

Анотація

У цій роботі проаналізовано методи розміщення даних у зображенні та розроблено програмний засіб для підвищення безпеки даних у зображенні та збереження структури контейнера. Програмний засіб розроблено в середовищі програмування Microsoft Visual Studio на базі Windows Form та застосовано мову програмування C#.

Ключові слова: стеганографія , контейнер, Microsoft Visual Studio, Windows Form, C#.

Abstract

In this work, the methods of placing data in the image are analyzed and a software tool is developed to improve the security of the data in the image and preserve the structure of the container. The software was developed in the Microsoft Visual Studio programming environment based on Windows Forms and the C# programming language was used.

Keywords: *steganography, container, Microsoft Visual Studio, Windows Form, C#.*

Вступ

Сьогодні у зв’язку зі стрімким розвитком інформаційних технологій виникають проблеми, пов’язані із захистом даних та приховуванням факту передачі [1, 2]. Проблема приховування інформації в нешкідливих контейнерах з метою секретної передачі полягає, наприклад, коли є потреба захистити мережевих записувачів, іноді змушує користувачів мережі використовувати методи комп’ютерної стеганографії (CS), щоб приховати правду. листування.

Для захисту даних, а точніше, для забезпечення, власне, факту захисту безпеки в цифровій стеганографії використовуються контейнери — цифрові об'єкти, в яких розміщується інформація, що часто призводить до структурних змін даних в контейнерах

Використання цифрової графіки у форматі стегоконтейнера залежить від таких причин:

— високий рівень поширення цифрової графіки;

— популярність і легкість обміну та публікації цифрових зображень в Інтернеті;

— зручний розмір контейнера з точки зору операцій з файлами (аудіофайли та відеофайли зазвичай у середньому більші за цифрові зображення);

— особливості системи зору людини, які не дозволяють візуально виявляти невеликі зміни в контейнері.

Однак більшість стеганографічних алгоритмів дозволяють приховати тільки невеликі обсяги інформації. Але на практиці часто виникає потреба у негласній передачі великих обсягів даних. Тому, дослідження у напрямку розробки програмного забезпечення важливо приховувати великі обсяги даних у відомих графічних форматах для подальшої їх передачі, є актуальними.

Детальне вивчення конкретних алгоритмів наведено в роботах Джордана (F. Jordan), Квісквотера (JJ Quisquater), E. Koxf (E. Koch), Куттера (M. Kutter), Дж. Жао (J. Zhao), Делейгла (J. - F. Delaigle), Боси (F. Bossen), Дармстедтера (V. Darmstaedter), Xcy (Chiou-Ting Hsu) і By (Ja-Ling Wu) та інших відомих вчених. Отже, з вищесказаного тема роботи є важливою та актуальною.

Результати дослідження

У сучасній стеганографії існує багато способів зберігання інформації в різних типах контейнерів. У цьому дослідженні увага зосереджена на вбудовуванні інформації саме у зображення. Методи молодших бітів, широкосмугові та статичні методи найбільш широко використовуються для цього типу контейнерів [3], тому запропоновано використовувати блоковий метод позиціонування контейнерного простору. Розроблений ними метод дозволяє досягти компромісу між стійкістю стеганосистеми до спотворень, якістю реалізації і, звичайно, обчислювальною складністю алгоритму [4]. Цей метод заснований на початковому тактильному (візуальному) відчутті та дозволяє регулювати розміщення блоків-контейнерів відповідно до їх поточного вмісту.

В загальному випадку, стеганографічну систему розроблюваного програмного засобу можна представити як комплекс таких складових [5]:

— обробник запитів — складова, яка забезпечує передачу інформації між додатком і користувачем для подальшої обробки;

— стегокодер — складова, яка відповідає за вбудовування даних в зображення;

— стегодетектор — складова, якаа використовується при виявленні вбудованих даних у зображення;

— обробник файлів — складова, яка відповідає за обробку файлів.

Схематично, наведені вище компоненти переставлені на рисунку 1.

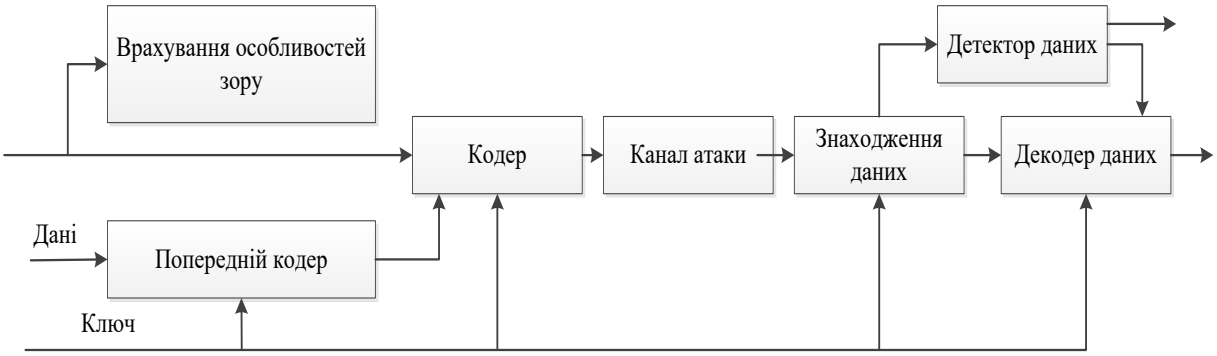

Рисунок 1 – Основні компоненти розроблюваного програмного засобу

Далі наведено архітектуру програмного засобу, який складається з наступних модулів:

— інтерфейс користувача;

— модуль отримання даних;

— модуль вбудовування прихованого повідомлення у зображення;

— модуль вилучення прихованого повідомлення.

Щодо інтерфейсу користувача, то він відображає форми при введенні даних користувачем і відображення результатів роботи.

Щодо модуля отримання даних, то він відповідає за обробку введених даних і передачу їх у інші модулі для виконання наступних розрахунків.

Далі у модулі вбудовування прихованого повідомлення зображення вбудовують послідовності біт прихованого зображення.

У модулі вилучення повідомлення виконується прогноз яскравості вибраного кольору, після чого вилучаються послідовності біт вбудованого повідомлення.

Вбудовування одного біта повідомлення відбувається в один піксель зображення, тоді може змінюватись яскравість червоного, синього, чи зеленого кольору, які вибирає користувач, інші кольори залишаються без змін. Далі розглядається приклад вибору користувачем синього кольору, отже:

R — яскравість червоного кольору;

G — яскравість зеленого кольору;

B —яскравість синього кольору;

m — вбудований біт ('1' чи '0');

x, y — координати пікселя.

Тоді $B^*_{x,y}$ — змінена залежно від біта, яка, вбудовується, яскравість синього кольору, обчислюється за наступною формулою

$$B^*_{x,y} = \begin{cases} B_{x,y} + 0.1 * (0.3 * R_{x,y} + 0.59 * G_{x,y} + 0.11 * B_{x,y}), \text{при } m_i = 1 \\ B_{x,y} - 0.1 * (0.3 * R_{x,y} + 0.59 * G_{x,y} + 0.11 * B_{x,y}), \text{при } m_i = 0 \end{cases}$$

При вилученні прогнозується відповідна яскравість синього кольору по сусіднім пікселям:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma},$$

де $\sigma = 1 \div 3$.

Для безпосереднього отримання повідомлення, яке приховується використовується формула:

$$m_i = \begin{cases} 1, \text{при } B^*_{x,y} > \overline{B_{x,y}} \\ 0, \text{при } B^*_{x,y} < \overline{B_{x,y}} \end{cases}.$$

У алгоритмі роботи передбачено забезпечення можливості користувача здійснювати приховування потрібних даних для подальшої їх передачі з врахуванням забезпечення захисту від витоку і несанкціонованого доступу із боку сторонніх користувачів.

Засіб надає можливість приховувати текстові дані у зображення. Це забезпечує зручність і ефективність використання розробки, тому, що різноманітні матеріали часто містять саме текстову і фото інформацію, яку доцільно зберігати разом для захисту від витоку.

Висновки

Проведено аналіз варіантів способів включення інформації в зображення.

Враховано результати попереднього аналізу можливих алгоритмів введення даних в зображення, а також використано метод розміщення блоків у просторовій області контейнера. Розроблено програмний засіб, що включає обробку основних компонентів: процесор запитів – компонент, який забезпечує передачу інформації між програмою та користувачем для подальшої обробки. ; стегокодер — це компонент, який відповідає за вбудовування даних у зображення; стегодетектор — це компонент, який використовується для виявлення вбудованих даних під час обробки файлу зображення.

Список використаної літератури

1. Heatherly R., Kantarcioglu M., Thuraisingham B. Preventing private information inference attacks on social networks. IEEE Transactions on Knowledge and Data Engineering. 2013. 25(8). P. 1849–1862.

2 Zheng L., Zhang Y., Thing V.L.L. A survey on image tampering and its detection in real-world photos. Journal of Visual Communication and Image Representation. 2019. 58. P. 380–399.

3. Ansari M.D., Ghrera S.P., Tyagi V. Pixel-based image forgery detection: A Review. IETE Journal of Education. 2014. 55(1). P. 40–46.

Азаров Олексій Дмитрович – доктор техн. наук, професор, завідувач кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Колесник Ірина Сергіївна – к.т.н., доцент, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Гонца Андрій Владиславович, ст. гр. 2КІ-22м, Вінницький національний технічний університет, Вінниця

Oleksyi D. Azarov – Dr. Sc., Professor, Head of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Iryna S. Kolesnyk – PHD, candidate of engineering sciences, associate professor of department of the computing engineering, Vinnytsya national technical university, Vinnytsya.

Gontsa V. Andrii – — student of group 2KI-22m, faculty of information technologies and computer engineering, Vinnytsia National Technical University