Нестерик Р.Р.
студент,
Науковий керівник: **Вовк Р.Б.**
кандидат технічних наук, доцент,
доцент кафедри програмного забезпечення автоматизованих систем,
Івано-Франківський національний технічний університет нафти і газу

ДОСЛІДЖЕННЯ ПЕРЕВАГ ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Впродовж останніх років майже вся сфера послуг перейшла на використання комп'ютерних мереж та IT-технологій, надзвичайний розвиток яких невпинно загострює питання інформаційної безпеки. Це зумовлюється необхідністю захисту інформації користувачів від втрат, до яких може призвести несанкціоноване використання даних, що знаходяться в інформаційних системах. Тому, в даний час, особливу увагу надають проблематиці ефективних методів захисту інформації, зокрема розробці методів захисту інтелектуальної цифрової власності.

Стеганографічні методи захисту інформації в цифрових системах, за своєю приналежністю, забезпечують більш високий рівень захисту (в порівнянні з криптографічними методами) через те, що захищені дані є невидимими в цифровому середовищі для несанкціонованих користувачів. Це складає принципову різницю між методами стеганографічного захисту та методами криптографічного захисту даних. Оскільки в криптографії користувач інформується про факт наявності захищеної інформації в цифровому зображенні чи в інших формах, то за допомогою стеганографічного захисту користувач, без певного роду шкідливих атак, не здатний виявити факт присутності таємної інформації в об'єкті. Дана властивість є ключовою у виборі методу захисту інформації яка суттєво розширює можливості стеганографії. Якщо ж необхідно здійснити захист від порушників, які ставлять за мету не тільки виявлення таємної інформації, а також її отримання та подальше використання, рекомендується використовувати методи стеганографії разом з криптографічним шифруванням. Проте не слід забувати, що необхідно узгодити статистичні характеристики даних, отримані на виході криптографічних алгоритмів з статистичними характеристиками контейнера в цифровому середовищі. Підхід повноцінної взаємодії стеганографії та криптографії дозволяє уникнути порушення законів, пов'язаних з передачею таємної та конфіденційної інформації, оскільки в багатьох країнах вважаються забороненими криптографічні способи приховання повідомлень, проте пропонований в даному дослідженні підхід дає свободу в реалізації захисту інформації.

Проведемо дослідження методів приховування інформації в нерухомих зображеннях та порівняємо їхню простоту у реалізації, а також стійкість до атак. Детально розглянемо принцип роботи методу заміни молодшого значущого біта (Least Significant Bit, LSB). Молодший значущий біт контейнера

(зображення, відео, аудіо) несе в собі найменший потік інформації і відомо те, що людина не здатна помітити зміни у даному біті. Фактично, LSB – це шум, тому його можна використовувати для вбудовування інформації шляхом заміни найменш значущих біт пікселів зображення бітами темного повідомлення [1]. Нехай задано 8-бітне зображення в градаціях сірого, де 00h (00000000b) позначає чорний колір, а FFh (11111111b) – білий. Усього є 256 градацій тобто 2 в 8 степені. Також маємо, що повідомлення складається з 1 байта – наприклад, 01101011b. При використанні 2 молодших бітів в описах пікселів, буде необхідно тільки чотири, з припущенням того, що вони чорного кольору. Тоді пікселі, що містять приховане повідомлення, будуть виглядати наступним чином: 00000001 00000010 00000010 00000011. Внаслідок цього колір пікселів зміниться наступним чином: в першого – на 1/255, другого і третього – на 2/255, і четвертого – на 3/255 [2].

Виділимо основні переваги даного методу:

1. Простота реалізації;
2. Стійкість до звичайних атак.

Також виділимо негативні сторони даного методу:

- Чутливість до розміру зображення;
- Знищення прихованого повідомлення при зміні контрастності та яскравості, а також при стисненні цифрового об’єкта;
- Неспроможність витримати атаки на стеганодетектор (на основі масштабування, тобто поворот чи відсічення зображення).

Розглянемо також ще один спосіб реалізації стеганографії – метод Куттера-Джордана-Боссена. При застосуванні даного методу вбудовування здійснюється шляхом модифікації яскравості синього кольору через те, що система зору людини в малій мірі чутлива до його зміни. Принцип вбудовування полягає в тому, що 1біт (повідомлення) поміщається в 1 піксель (контейнер), а секретний ключ задає координати пікселів, в які буде вбудовуватись інформація. Використаємо RGB модель, в якій червоний та зелений кольори залишаються без змін, а контраст синього змінюється згідно формули:

$$B^*_{x,y} = \begin{cases} B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 1 \\ B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 0 \end{cases}, \text{де } \lambda Y_{x,y} = 0.29890 \cdot R_{x,y} + 0.58662 \cdot G_{x,y} + 0.11448 \cdot B_{x,y} - \text{яскравість пікселя}$$

Для декодування виконується передбачення значення яскравості вихідного синього кольору на основі його сусідів з використанням наступного співвідношення:

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

де σ = 1÷3 – розмір області, по якій буде прогнозуватись яскравість [3].

Даний метод є дещо складнішим в порівнянні з попереднім, проте в ньому є ряд переваг яких немає в LSB та інших методах стеганографії, а саме:

1. Висока пропускна здатність;

2. Висока стійкість до несанкціонованого доступу та до частого декодування;

3. Стійкість до знищення молодших бітів контейнера та до атаки стиснення;

4. Висока стійкість до атак на стеганодетектор.

Недоліком даного методу є те, що при витягуванні зашифрованої інформації можна втратити частину даних. Проте даний недолік можна усунути використанням кодування, яке є стійким до перешкод.

Описані вище методи з високою ймовірністю виконують задачі, які поставлені перед ними. Вибираючи який з даних методів є більш ефективним в плані вбудовування прихованої інформації, то метод Куттера-Джордана-Боссена є більш ефективним, тільки через вищий рівень захисту вбудованої інформації та є менш вразливим до атак. Однак метод LSB, незважаючи на свої недоліки, є популярнішим та простішим в реалізації.

З викладеного вище слідує, що методи, які реалізовують комп'ютерну стеганографію, є близькими до ідеально-завершених, проте з практичної точки зору не є надійними на 100%. Отже, в даній роботі розглянуто основні способи реалізації стеганографічного захисту, а також охарактеризовано його базові принципи роботи, виділено переваги та недоліки основних методів стеганографії, що спрощує вибір методу, який найкраще відповідає поставленій задачі. Також розглянуто підхід симбіозу стеганографії та криптографії, який дає змогу без особливих зусиль приховувати інформацію.

Таким чином, в проведеному дослідженні розглянуто важливі аспекти захисту цифрової інформації шляхом використання стеганографічних методів. Перспективою подальших досліджень є розробка нових методів захисту цифрової інформації, з використанням стеганографії в симбіозі з іншими методами чи алгоритмами захисту.

Список використаних джерел:

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.

2. Стеганографія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Стеганографія. – Перевірено: 14.10.15.

3. Конахович Г. Ф., Пузыренко А. Ю. «Компьютерная стеганография. Теория и практика». – М.: МК-Пресс, 2006. – 288 с.